MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 501 -

POR LA CUAL SE APRUEBA Y PONE EN VIGENCIA LA GUIA DE ESTANDARES TECNOLOGICOS Y LINEAMIENTOS DE SEGURIDAD PARA LA HABILITACION Y AUDITORIA A PRESTADORES DE SERVICIOS DE CERTIFICACION.

Asunción, 28 de ABRIL de 2016

VISTO: El Memorándum DAL N° 16 de fecha 19 de junio de 2015, de la Dirección de Asuntos Legales de la Dirección General de Firma Digital y Comercio Electrónico remitido a la Subsecretaria de Estado de Comercio, en el cual solicita la Resolución que apruebe la Guía de Estándares Tecnológicos y lineamientos de seguridad para la habilitación y auditoria a Prestadores de Servicios de Certificación; y

CONSIDERANDO: La Ley N° 4017/10 "De Validez Jurídica de la Firma Electrónica, Firma Digital, Los Mensajes de Datos y el Expediente Electrónico".

El Decreto N° 7369/11 "Por el cual se aprueba el Reglamento General de la Ley N° 4017/10".

La Ley N° 4610/12 "Que modifica y amplia la Ley N° 4017/10 "De Validez Jurídica de la Firma Electrónica, Firma Digital, Los Mensajes de Datos y el Expediente Electrónico".

Que el Ministerio de Industria y Comercio es la Autoridad de Aplicación de las normativas mencionadas, como tal facultado a autorizar la operación de entidades de certificación en el territorio nacional, velar por el adecuado funcionamiento y la eficiente prestación del servicio por parte de las entidades de certificación y el cabal cumplimiento de las disposiciones legales y reglamentarias de la actividad.

Que el Ministerio de Industria y Comercio a través de la Dirección General de Firma Digital y Comercio Electrónico, ha elaborado la referida Guía de conformidad a los términos del artículo 39 inciso b) y e) de la Ley N° 4610/12, el artículo 19 del Decreto Reglamentario N° 7369/11 y reglamentaciones vigentes.

La necesidad de puntualizar y clarificar los requerimientos generales consignados en la legislación, en la política y declaración de prácticas de certificación, para la habilitación, auditoría e inspecciones a los interesados en constituirse en prestadores de servicios de certificación o habilitados, en su caso.

Que esta Guía orientará a los interesados en constituirse en Prestadores de Servicios de Certificación respecto al cumplimiento de los estándares internacionales y disposiciones de carácter técnico y legal para ser habilitado por el Ministerio de Industria y Comercio, así como respecto a las auditorías e inspecciones a que sean sometidos por la autoridad de aplicación, una vez habilitados.

ES COPIA FIEL DEL ORIGINAL
MINISTERIO DE INDUSTRIA Y COMERCIO - Secretaría General -

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Econ. Expidio Palacios
Secretario General

MINISTERIO DE INDUSTRIA
Y COMERCIO

Resolución N° 501.-

POR LA CUAL SE APRUEBA Y PONE EN VIGENCIA LA GUIA DE ESTANDARES TECNOLOGICOS Y LINEAMIENTOS DE SEGURIDAD PARA LA HABILITACION Y AUDITORIA A PRESTADORES DE SERVICIOS DE CERTIFICACION.

El Dictamen Jurídico N° 536 de fecha 02 de setiembre de 2015, emitido por la Dirección General de Asuntos Legales, no opone reparos legales a fin de proseguir con los trámites administrativos pertinentes para la promulgación de la Resolución.

POR TANTO, en uso de sus atribuciones legales

EL MINISTRO DE INDUSTRIA Y COMERCIO

R E S U E L V E:

Art. 1°.- Aprobar y poner en vigencia la Guía de Estándares Tecnológicos y Lineamientos de Seguridad a ser considerados, en el proceso de habilitación, y en los procesos de auditorías e inspecciones que se lleven a cabo a los Prestadores de Servicios de Certificación habilitados, cuyo texto se anexa y forma parte de la presente Resolución.

Art. 2°.- Disponer que la presente Resolución entre a regir a partir del 01 de enero de 2017.

Art. 3°.- Comunicar a quienes corresponda y cumplida, archivar.

JOSE LUIS RODRIGUEZ TORNACO
Ministro Sustituto

ES COPIA FIEL DEL ORIGINAL

Econ. Expidio Palacios
Secretario General

JLRT/EP/pm

ANEXO

INTRODUCCIÓN

El presente manual ha sido redactado con la finalidad de definir los estándares y lineamientos de seguridad para la habilitación y auditoría de los Prestadores de Servicios de Certificación y a la vez orientar a las entidades que desean convertirse en Prestadores de Servicios de Certificación, y formar parte de la Infraestructura de Clave Pública del Paraguay (PKI PY) y mantenerse como tal el tiempo que preste el servicio.

El contenido del presente documento guía al solicitante con respecto a la aplicación de las leyes y los estándares que han de ser considerados al momento de analizar el cumplimiento de los requisitos tecnológicos, de seguridad y confianza.

1. OBJETO Y CAMPO DE APLICACIÓN

El propósito de la presente guía es orientar al interesado en constituirse en Prestador de Servicios de Certificación con relación a la aplicación de los estándares y directrices que serán consideradas al momento de analizar el cumplimiento de los requisitos tecnológicos, de seguridad y confianza que exige la normativa vigente para constituirse en Prestador de Servicios de Certificación (PSC) y formar parte de la Infraestructura de Clave Pública del Paraguay (PKI PY).

2. REFERENCIASNORMATIVAS

- **a.** Ley N° 4017/10 "Validez Jurídica de la Firma Electrónica, La Firma Digital, Los Mensajes de Datos y El Expediente Electrónico".
- **b.** Decreto N° 7369/11 que reglamenta la Ley N° 4017/10
- **c.** Ley N° 4610/12 "Que amplía y modifica parcialmente la Ley N° 4017/10".
- **d.** Norma Paraguaya NP-ISO/IEC 27001. Tecnología de la Información – Técnicas de Seguridad – Sistemas de seguridad de la Información – Requisitos.
- **e.** ISO/IEC 27005:2011 Tecnología de Información. Técnicas de seguridad. Gestión del riesgo en la seguridad de la información.
- **f.** ISO 22301:2012. Sistema de Gestión de Continuidad del Negocio. Requerimientos.
- **g.** FIPS PUB 140-2 Security Requirements for Cryptographic Modules, (Diciembre
- **h.** 2002).
- **i.** RFC 5280, "Internet X.509 Public Key Infrastructure Certificate and Certificate. Revocation List (CRL).

Abog. Rocío Rolón A. DIRECTOR GENERAL Firma Digital y Comercio Electrónico

ES COPIA FIEL DEL ORIGINAL

MINISTERIO DE INDUSTRIA Y COMERCIO - Secretaría General

Econ. Expidio Palacios
Secretario General

j. ISO/IEC 9594-8: 2014 Information Tecnology – Open Systems Interconnection – The Directory: Public Keyand Attribute Certificate Frameworks.

k. ITU-T Rec. X.509 Tecnología de la información. Interconexión de sistemas abiertos – El directorio: Marcos para certificados de clave pública y atributos.

l. RFC 3647. "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

m. ETSI TS 102 042 European Telecommunications Standards Institute. Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.

n. RFC 6960. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.

o. Política de Certificación de la Infraestructura de Clave Pública del Paraguay.

p. Declaración de Prácticas de Certificación de la Infraestructura de Clave Pública del Paraguay

3. DEFINICIONES Y TERMINOLOGÍAS

A los efectos de esta guía, se establecen las siguientes definiciones y terminologías:

- **Autoridad de Aplicación (AA):** Ministerio de Industria y Comercio a través de la Dirección General de Firma Digital y Comercio Electrónico, dependiente del Viceministerio de Comercio. Órgano Regulador competente designado por Ley, establecido por el Artículo 38 de la Ley N° 4610/12 que modifica y amplía la Ley N° 4017/10 "De Validez Jurídica de la Firma Electrónica, La Firma Digital, Los Mensajes de Datos y El Expediente Electrónico".

- **Autoridad Certificadora (CA):** Entidad que presta servicios de emisión, gestión, revocación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de una RA. En el marco de la PKI Paraguay, son Autoridades Certificadoras, la CA Raíz del Paraguay y el PSC.

- **Autoridad Certificadora Raíz (CA Raíz):** Es la Autoridad de Certificación Raíz de la PKI Paraguay, cuya función principal es habilitar al PSC y emitirle certificados digitales. Posee un certificado auto firmado y es a partir de allí, donde comienza la cadena de confianza.

- **Autoridad de Registro (RA):** Entidad responsable de la identificación y autenticación de titulares de certificados digitales, la misma no emite ni firma certificados. Una RA puede ayudar en el proceso de solicitud del certificado, en el proceso de revocación o en ambos. La RA no necesita ser un organismo separado sino que puede ser parte de la CA.

Abog. Yodys Rolón A. DIRECTOR GENERAL

ES COPIA FIEL DEL ORIGINAL

MINISTERIO DE INDUSTRIA Y COMERCIO Secretaría General

Econ. Expidio Palacios
Secretario General

- **Certificado Digital (CD):** Es un documento electrónico, generado y firmado por una CA legalmente habilitada para el efecto, el cual vincula un par de claves con una persona física o jurídica confirmando su identidad.
- **Clave Privada:** Es una de las claves de un sistema de criptografía asimétrico que se emplea para generar una firma digital sobre un mensaje de datos y es mantenida en reserva por el titular de la firma digital.
- **Clave Pública:** Es la otra clave del sistema de criptografía asimétrica, que es usada por el destinatario de un mensaje de datos para verificar la firma digital puesta en dicho mensaje. La clave pública puede ser conocida por cualquier persona.
- **Compromiso:** Violación de la seguridad de un sistema a raíz de una posible divulgación no autorizada de información sensible.
- **Contrato o Acuerdo de Suscriptores:** Es un acuerdo entre la CA Raíz y el PSC, y entre el PSC y el usuario final, que establece los derechos y responsabilidades de las partes con respecto a la emisión y gestión de los certificados. Éste acuerdo, requiere la aceptación explícita tanto del PSC, como del suscriptor, respectivamente.
- **Datos de activación:** Valores de los datos, distintos a las claves, que son requeridos para operar los módulos criptográficos y que necesitan estar protegidos.
- **Declaración de Prácticas de Certificación (CPS):** Declaración de las prácticas que emplea una CA al emitir certificados y que define la infraestructura, políticas y procedimientos que utiliza la CA para satisfacer los requisitos especificados en la CP vigente.
- **Delta CRL:** Partición del CRL, dentro de una unidad de tiempo, que contiene los cambios realizados al CRL base desde su última actualización.
- **Estándares Técnicos Internacionales:** Requisitos de orden técnico y de uso internacional que deben observarse en la emisión de firmas electrónicas y en las prácticas de certificación.
- **Firma Digital:** Es una firma electrónica certificada por un prestador habilitado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincula únicamente al mismo y a los datos a lo que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría.

ES COPIA FIEL DEL ORIGINAL

Abog. Fátima Rolón A.
Dirección General
Firma Digital y Comercio Electrónico

MINISTERIO DE INDUSTRIA Y COMERCIO
Secretaría General

Econ. Expidio Palacios
Secretario General

- **Firmante, suscriptor o signatario:** Es toda persona física o jurídica titular de la firma electrónica o digital. Cuando el titular sea una persona jurídica, ésta es responsable de determinar las personas físicas a quienes se autorizarán a administrar los datos de creación de la firma electrónica o digital.
- **Infraestructura de Clave Pública (PKI):** Es un conjunto de personas, políticas, procedimientos y sistemas informáticos necesarios para proporcionar servicios de autenticación, integridad y no repudio, mediante el uso de criptografía de claves públicas y privadas y de certificados digitales, así como la publicación de información, consultas de vigencia y validez de los mismos.
- **Lista de certificados revocados (CRL**): Lista emitida por una CA, publicada periódicamente y que contiene los certificados que han sido revocados antes de sus respectivas fechas de vencimiento.
- **Módulo de Seguridad de Hardware (HSM, Hardware Security Module**): Dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas.
- **No Repudio:** Refiere que la posesión de un documento electrónico y la firma digital asociada al mismo, será prueba efectiva del contenido y del autor del documento.
- **Par de claves:** Son las claves privada y pública de un criptosistema asimétrico. La clave privada y la clave pública están relacionadas matemáticamente y poseen ciertas propiedades, entre ellas que es imposible deducir la clave privada de la clave pública conocida.
- **Perfil del certificado:** Especificación del formato requerido para un tipo particular de certificado (incluyendo requisitos para el uso de los campos).
- **Política de Certificación: (CP)** Documento en el cual la CA, define el conjunto de reglas que indican la aplicabilidad de un certificado a una comunidad particular y/o una clase de aplicaciones con requisitos comunes de seguridad.
- **Prestador de Servicios de Certificación (PSC):** Entidad habilitada ante la AA, encargada de operar una CA en el marco de la PKI Paraguay. El PSC debe contar con un certificado digital emitido por la CA Raíz y solo podrá emitir certificados a usuarios finales.
- **Repositorio:** Sitio principal de internet confiable y accesible, mantenido por la CA con el fin de difundir su información pública.
- **Token de seguridad:** Dispositivo electrónico donde se almacena de forma segura la clave privada del suscriptor.

ES COPIA FIEL DEL ORIGINAL
MINISTERIO DE INDUSTRIA Y COMERCIO
Secretaría General

Abog. Rocío Rolón A.
DIRECTORA GENERAL
Firma Digital y Comercio Electrónico

Econ. Expidio Palacios
Secretario General

- **Servicio OCSP:** Permite utilizar un protocolo estándar para realizar consultas en línea al servidor de la CA sobre el estado de un certificado.
- **Solicitud de Firma de Certificado (CSR):** Es una petición de certificado digital que se envía a la CA. Mediante la información contendida en el CSR, la CA, puede emitir el certificado digital una vez realizadas las comprobaciones que correspondan.
- **Suscriptor:** Persona física o jurídica titular de un certificado digital emitido por una CA.
- **Usuario final:** Persona física o jurídica que adquiere un certificado digital de un PSC.

4. SIMBOLOS Y ABREVIATURAS

BCP: Por sus siglas en inglés, Plan de Continuidad del Negocio (Business Continuity Plan).
CA: Por sus siglas en inglés, Autoridad de Certificación.
CP: Por sus siglas en inglés, Política de certificación.
CPS: Por sus siglas en inglés, Declaración de prácticas de Certificación.
CRL: Por sus siglas en inglés, Lista de certificados revocados.
DGFDYCE: Dirección General de Firma Digital y Comercio Electrónico.
DoS: Denegación de servicio (Denial of service).
DRP: Por sus siglas en inglés, Plan de Recuperación de Desastres (DesasterRecovery Plan).
MIC: Ministerio de Industria y Comercio.
OCSP: Por sus siglas en inglés; Protocolo en línea del estado del Certificado (Online Certificate Status Protocol).
PKI PY: Por sus siglas en inglés, Infraestructura de Clave Pública del Paraguay.
PSC: Prestador de Servicios de Certificación.
RA: Por sus siglas en inglés, Autoridad de registro.
RUC: Registro único del contribuyente.

5. CRITERIOS DE HABILITACIÓN

5.1. Principio Básico

A través de esta guía se pueden conocer y analizar, con el detalle y rigurosidad que exige la normativa vigente, los aspectos que deben ser verificados en el área tecnológica, de seguridad y confianza, lo que permitirá definir un criterio preciso sobre su capacidad para lograr un servicio de certificación digital seguro y mantener en el tiempo la habilitación como PSC.

ES COPIA FIEL DEL ORIGINAL
MINISTERIO DE INDUSTRIA Y COMERCIO - Secretaría General
Abog. Hugo Rolón A.
Dirección Jurídica
Lcdo. Expidio Palacios
Secretario General

5.2. Consideraciones Generales

Los criterios de habilitación están definidos en base a los requisitos y obligaciones definidos por la Ley N° 4017/10 "De Validez Jurídica de la Firma Electrónica, La Firma Digital, Los Mensajes de Datos y El Expediente Electrónico", la Ley N° 4610/12 que la modifica parcialmente y la amplía, el Decreto N° 7369/11 y las Reglamentaciones establecidas por el Ministerio de Industria y Comercio (MIC) en su calidad de Autoridad de Aplicación.

Con el fin de crear confianza a los usuarios con relación al servicio de certificación digital y generar las condiciones necesarias para el desarrollo de la actividad, se pone a disposición los requisitos que se deben cumplir para ser habilitado como PSC en la República del Paraguay.

Los requerimientos del proceso de habilitación deben garantizar la compatibilidad de la Infraestructura de Clave Pública del Paraguay con los estándares internacionales, permitiendo así la interoperabilidad entre los sistemas.

Los niveles de exigencia del proceso de habilitación deben ajustarse a las mejores prácticas y los estándares internacionales.

Se considera fundamental promover el desarrollo tecnológico de los servicios de certificación digital, sin preferencia hacia una tecnología en particular. Además el PSC podrá introducir cambios tecnológicos siempre que cumpla con la normativa establecida, previa notificación al MIC.

La realización de un proceso de habilitación requiere de información sensible del interesado en ser PSC.

En ese sentido, el MIC se compromete a no usar ni divulgar la información proporcionada por el PSC, clasificada como confidencial, más que para los fines propios del procedimiento de habilitación. Este compromiso es extensible a todo organismo y persona que intervenga en el proceso de habilitación.

El contenido de los criterios considerados en el proceso de habilitación, puede cambiar en el tiempo, dependiendo de los avances de la tecnología y consideraciones de seguridad nacional. Si el cambio es considerado significativo, el proceso de revisión incorporará consultas con el sector de interés y debe ser validado por MIC.

Todo PSC habilitado debe ser notificado de los cambios de este documento. Si existiera alguna duda respecto a la actualización de estos criterios, deberá consultarse al MIC.

Econ. Expidio Palacios
Secretario General

Los lineamientos establecidos en este documento se basan en estándares internacionales que permiten ofrecer de forma segura y confiable servicios de certificación digital.

Conforme a las disposiciones de la normativa vigente, se establece un procedimiento de habilitación que involucra los siguientes componentes:

- **MIC:** El proceso de habilitación del PSC es realizado por el MIC a través de su organismo técnico la Dirección General de Firma Digital y Comercio Electrónico (DGFDYCE), la que podrá contar con el apoyo de expertos, para la ejecución de las tareas de evaluación. La DGFDYCE además, debe velar por el cumplimiento de los requisitos y obligaciones que se observaron al momento de otorgarse la habilitación y que deberán mantenerse durante la vigencia de la misma. Para ello, puede requerir información, ordenar inspecciones ordinarias o extraordinarias, auditorías a las instalaciones del PSC, sin previo aviso, con su personal o por medio de auditores externos.
- **Auditor:** Personal técnico, capacitado y experimentado encargado de realizar evaluación en el proceso de la habilitación o de la auditoría. Esta función podrá ser desempeñada por técnicos del MIC o por terceros autorizados para ese efecto.
- **Prestador de Servicios de Certificación (PSC)** Persona jurídica habilitada por el MIC para prestar Servicios de Certificación Digital dentro de la Infraestructura de Clave Pública del Paraguay.
- **Registro del PSC habilitado** Registro público electrónico que mantiene el MIC, que contiene los datos relacionados al PSC habilitado.
- **Estándares Técnicos** Conjunto de estándares internacionales vigentes y establecidos por el MIC y que debe cumplir el PSC para ser habilitado de conformidad al Artículo 19 del Decreto Reglamentario N° 7369/11.
- **Requisitos** requerimientos técnicos y legales que debe cumplir el PSC para ser habilitado por el MIC y que se encuentran establecidos en el Artículo 8 del Decreto Reglamentario N° 7369/11, Artículo 28 de la Ley N° 4017/10 y demás disposiciones vigentes sobre la materia.

Los estándares tecnológicos y lineamientos de seguridad a aplicar para la habilitación como PSC se detallan a continuación en las consideraciones específicas.

5.3. Consideraciones Específicas

5.3.1. Estructura e información del Certificado Digital

Abog. Rosa Rolón A. Dirección General Firma Digital y Comercio Electrónico

ES COPIA FIEL DEL ORIGINAL

MINISTERIO DE INDUSTRIA Y COMERCIO - Secretaría General

Econ. Expidio Palacios
Secretario General

5.3.1.1 **Objetivo:** Comprobar los aspectos que dispone la Ley N° 4017/10 con relación a lo delineado en el estándar ITU-T Rec. X.509, contenidos mínimos, incorporación de los requisitos mínimos obligatorios, límites y atributos del certificado digital.

5.3.1.2 **Descripción:** La estructura de datos que conforma el certificado Digital emitido por el PSC debe estar conforme al estándar ITU-T Rec. X.509.

El certificado digital emitido por el PSC debe contener al menos los siguientes datos:

- Un código de identificación único del certificado.
- Identificación del PSC, con indicación de su razón social, RUC, código de país.
- Los datos de la identidad del suscriptor, entre los cuales deben necesariamente incluirse su nombre o razón social, documento de identidad o RUC y finalidad del certificado según CP 7.1.
- Plazo de vigencia (fecha de emisión y vencimiento).
- El PSC debe incorporar en sus certificados su RUC y la identificación del suscriptor de acuerdo a la estructura e identificadores que se especifica en la CP de la PKI PY.
- El PSC debe indicar en forma explícita, que el certificado emitido corresponde a una política de certificados con los límites de uso. Esta indicación debe quedar inserta en el campo "Políticas de Certificación (Certificate Policies)" de las extensiones del certificado del formato X.509 versión 3.
- El PSC interesado debe estructurar los certificados que emite, de forma que los atributos adicionales que introduce, así como la incorporación de límites al uso del certificado, no impidan la lectura del mismo ni su reconocimiento por terceros de la Infraestructura de Clave del Paraguay (PKI PY.).
- Los límites de uso que se incorporen en los certificados, deben ser reconocibles por terceros de la PKI PY.
- Los datos de creación de firma del PSC para emitir certificados, no deben ser utilizados más allá de lo establecido en la CP aprobada por el MIC.
- El perfil del certificado debe estar acorde a lo establecido en el punto 7.1. de la CP del PSC y de la CP de la PKI PY.
- El tamaño de las claves debe ser el establecido en la CP.

MINISTERIO DE INDUSTRIA Y COMERCIO - Secretaría General - ES COPIA FIEL DEL ORIGINAL

Abog. Rodys Rolón A. DIRECTOR GENERAL Firma Digital y Comercio Electrónico

5.3.1.3 **Estándares de Evaluación**

- ITU-T Rec. X.509 / ISO/IEC 9594-8
- RFC 5280

Lcdo. Expidio Palacios
Secretario General

5.3.1.4 Documentación Solicitada

- Modelos de Certificados digitales, emitidos por el PSC en evaluación.
- Modelo de la solicitud de firma del certificado (CSR).

5.3.1.5 Detalles de Evaluación

Aspectos	Evaluación
Conformidad con el estándar ITU-T Rec. X.509	Se verificará que la estructura básica del certificado esté conforme a la norma que rige la materia y que la gramática utilizada tanto en la estructura básica como en las extensiones obligatorias, puedan ser leídas por cualquier aplicación que cumpla el estándar ITU-T Rec. X.509. V3.
Contenido básico del certificado digital emitido por el PSC.	Se confirmará que el certificado contiene la siguiente información: a. Un código de identificación único del certificado. (Serial number) b. Identificación del PSC, con indicación de su razón social, RUC, código de país, de acuerdo a la estructura e identificadores que se especifica en la CP de la PKI PY. *(issuer)* c. Los datos de la identidad del suscriptor, entre los cuales deben necesariamente incluirse su nombre o razón social, documento de identidad o RUC y finalidad del certificado según el punto 7.1 de la CP (subject). d. Plazo de vigencia (fecha de inicio y de vencimiento) validity (notBefore, notAfter). e. El Algoritmo de firma (signature algorithm). f. La versión.(versión). g. La clave pública del suscriptor. (Public Key). h. El PSC debe indicar en forma explícita, que el certificado emitido corresponde a una política de certificados con los límites de uso. Esta indicación debe quedar inserta en el campo "Políticas de Certificación (Certificate Policies)" de las extensiones del certificado del formato X.509 versión 3. i. Las extensiones deben ser acordes a lo establecido en la CP. El perfil del certificado debe estar acorde a lo establecido en punto 7.1. de la Política de Certificación del PSC y de la CP de la PKI PY.
Método de incorporación de identificación del suscriptor	Se verificará que el PSC incorpore en sus certificados el identificador indicado, por ejemplo en caso de que el suscriptor sea persona jurídica se debe incluir el RUC. Según lo señalado en el punto3.1 de la CP.
Lectura y reconocimiento del contenido mínimo cuando existen atributos adicionales en el certificado	Se validará que el PSC estructure sus certificados, de forma que los atributos adicionales que introduzca con el fin de incorporar límites al uso del certificado, si los hay, no impidan la lectura ni su reconocimiento por terceros.
Reconocimiento de límites de uso del certificado digital por terceros	Se verificará que el PSC estructure sus certificados de manera que los límites de uso, si los hay, sean reconocibles por terceros.
Uso de clave pública acreditada	Se verificará que los datos de creación de firma del PSC para emitir certificados no sean utilizados más allá de lo establecido en la CP aprobada por el MIC.
Algoritmos de firma	Se validará que el PSC utilice algoritmos de firma que provean el adecuado nivel de seguridad aprobado por el MIC tanto para su propia firma como para la firma del suscriptor. El algoritmo de firma debe ser Sha256 RSA.
Tamaño de las claves	Se comprobará que el PSC utilice el tamaño de clave pública y privada, mínimo 4096 bits para su propia firma y 2048 bits para la firma del suscriptor.

Aspectos	Evaluación
Funciones Hash	Se verificará que el PSC utilice funciones hash de última generación que provean el nivel de seguridad, tanto para su propia firma como para la firma del suscriptor. El algoritmo hash para firma debe ser Sha256.

5.3.2. Estructura de la Lista de Certificados Revocados y Servicio OCSP

5.3.2.1 **Objetivo:** Verificar que las listas de certificados revocados tengan el formato y contenido especificado en el estándar, y permita al suscriptor identificar plenamente al PSC emisor de la CRL.

Verificar que el estado de los certificados tengan el formato y contenido especificado en el estándar, y permita al usuario identificar plenamente el estado del certificado emitido por el PSC emisor.

5.3.2.2 **Descripción:** La lista de certificados revocados (CRL) debe contener la información y estructura que especifica el estándar ISO/IEC 9594-8 y del RFC 5280.

La lista debe contener al menos la identificación del emisor, fecha de su emisión e identificación de los certificados revocados a dicha fecha.

La lista podría ser almacenada y enviada en medios inseguros, por lo que debe estar debidamente firmada por el PSC emisor.

El servicio en línea de estado de los certificados (OCSP) debe contener la información y estructura que especifica el estándar RFC 6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol"

5.3.2.3 **Estándares de Evaluación**

- ITU-T Rec. X.509 / ISO/IEC 9594-8
- RFC 5280
- RFC 6960

5.3.2.4 **Documentación Solicitada**

- CP y CPS del PSC.
- CRL emitida por el PSC en evaluación y el certificado digital de la CA que la emite.
- Respuesta a Consulta de Estado de Certificado al Servicio OCSP del PSC.

Abog. Carlos Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Econ. Expidio Palacios
Secretario General

5.3.2.5 **Detalles de evaluación**

Aspectos	Evaluación
Contenido Mínimo	Se verificará que la CRL contenga la siguiente información: a) Versión. Debe tener el valor 2. b) Nro. CRL: número que identifica de forma única a cada CRL emitida por el PSC c) Algoritmo de firma. Este campo debe contener la identificación del algoritmo de firma utilizado, siguiendo el RFC 5280. El algoritmo de firma debe ser como mínimo SHA256RSA d) Nombre del emisor. Este campo debe contener el nombre de la entidad que emitió y firmó la CRL. e) Fecha efectiva: este campo debe contener la fecha y hora en que fue emitida la CRL. f) Próxima actualización: se deberá incluir en este campo la fecha en que se emitirá la próxima CRL. g) Emitir puntos de distribución: en este campo debe incluir el url de donde descargar la CRL. h) Identificador de clave de entidad emisora: este campo contiene el hash de la clave pública del PSC. i) Certificados revocados: este campo debe contener los números de serie de los certificados revocados por el emisor, indicando también la fecha y hora de revocación correspondiente, y el motivo de la revocación. Se verificará que el OCSP del PSC este implementado de acuerdo al estándar RFC 6960 en sus mecanismos de: a) Petición de validación b) Respuesta a la validación.
Comprobación de firma	Se comprobará que la CRL esté debidamente firmada por el PSC.
Mecanismo de Petición de Validación y Respuesta a la Validación	Se verificará que el servicio OCSP tenga implantado los mecanismos de Petición de Validación y Respuesta a la Validación

5.3.3 **Registro de Acceso Público.** (Servicios, contenido y accesibilidad electrónica del sistema público de información del PSC).

5.3.3.1 **Objetivo**: Asegurar el acceso a información relevante descriptiva del sistema a los suscriptores y terceros de manera permanente.

5.3.3.2 **Descripción**

Se verificará que el PSC:

- Garantice la existencia de un servicio seguro de consulta remota de un registro de certificados revocados.
- Garantice la existencia de un servicio de consulta de estado de certificados on line (Protocolo OCSP).

- Garantice la existencia de un repositorio seguro donde se puedan acceder a los documentos y certificados establecidos en la normativa.
- Provea acceso al repositorio a los suscriptores y partes interesadas por medios electrónicos de manera continua y regular.
- Use sistemas y productos confiables que garanticen la seguridad de su sistema de difusión de información.
- Cuente con procedimientos para informar a los suscriptores las características generales de los procesos de creación y verificación de firma digital, así como de las reglas sobre prácticas de certificación que el PSC se comprometa a utilizar en la prestación del servicio.
- Tenga procedimientos para dejar sin efecto definitivamente (revocar) los certificados.
- Cuente con procedimientos para publicar y actualizar en su sitio de internet la información de acceso electrónico, las resoluciones del MIC que le afecten, la CP, la CPS y todos los documentos establecidos en la normativa. Esto debe realizarse como mínimo en los sitios de dominio público registrados durante el proceso de habilitación.
- Provea de los manuales y software (controladores) necesarios para la operación de los dispositivos de firma segura que proporcione a sus usuarios.

5.3.3.3 **Estándares de Evaluación**

- No aplica

5.3.3.4 **Documentación Solicitada**

Documento descriptivo que contenga al menos la siguiente información:

- Detalle del sitio Web donde publicará la información.
- Descripción de la tecnología utilizada.
- Disponibilidad, accesibilidad, conexión, esquemas y diagramas de funcionamiento.
- Medidas de seguridad implementadas para asegurar que solo personal autorizado pueda modificar el sitio.
- Sitio web de prueba con las funcionalidades requeridas.
- Documento de test de penetración, realizado por una empresa auditora calificada.
- Documento descriptivo de la implementación del protocolo OCSP.

ES COPIA FIEL DEL ORIGINAL

Abog. Fátima Rolón A.
DIRECTORA GENERAL
Firma Digital y Comercio Electrónico

Econ. Expidio Palacios
Secretario General

5.3.3.5 Detalles de la Evaluación

Aspectos	Evaluación
Existencia y contenido mínimo del Sitio Web de información pública	El PSC debe mantener un sitio de acceso electrónico, con información relevante para los suscriptores y las partes que confían. Al menos debe contener los siguientes documentos: a) CP Y CPS que implementan. b) Certificado de la CA Raíz c) Certificado del PSC d) Copia de Lista de certificados revocados actualizada cada semana o cuando surja la revocación del certificado del suscriptor. La latencia de publicación del certificado debe ser no mayor a 1 hora. e) Publicación del Delta CRL cada 24hs. (si es que esta implementado). f) Lista de certificados vigentes y revocados. g) La proforma de contrato de suscriptor. h) Las resoluciones que habilitan, suspenden o revocan al PSC. i) La información relevante de la última auditoría que fueran objeto. j) Leyes, decretos, reglamentos y resoluciones que rigen la actividad de la PKI PY. k) Identificación, domicilio y medio de contacto.
Disponibilidad de la Información y servicio	Se debe asegurar una disponibilidad del sitio no menor al 99% anual y un tiempo programado de inactividad máximo de 0,5% anual. Para esto se verificará la existencia de mecanismos redundantes o alternativos de conexión y sitios de emergencia que se levanten manual o automáticamente en caso de desastres.
Seguridad	Se debe proteger la integridad y disponibilidad de la información mediante el uso de tecnología y medidas de seguridad tanto físicas como lógicas que reduzcan los riesgos y consecuencias de ataques maliciosos tanto internos como externos en contra del sitio. El repositorio debe contar con un certificado SSL. Se debe realizar un test de penetración anualmente a la página Web.
Servicio de Validación en línea de certificados	Se debe tener implementado el servicio OCSP para validación de certificado.

5.3.4 Revisión de la Evaluación de Riesgos y Amenazas

5.3.4.1 **Objetivo:** Determinar la consistencia del análisis de riesgos y amenazas del plan de negocios del PSC.

5.3.4.2 **Descripción**

Dado que la base principal en que se sustenta el servicio del PSC es la "confianza", el requerimiento fundamental para un PSC es demostrar una clara comprensión de las amenazas de seguridad enfrentadas por el negocio y poder mostrar planes efectivos para reducir el riesgo residual a un nivel aceptable.

El objetivo principal de un proceso de Gestión del riesgo en una organización debe ser proteger la organización, su capacidad de cumplir con su misión y no impactar en forma significativa los objetivos organizacionales.

Abog. Rocío Rolón A. DIRECTORA GENERAL Firma Digital y Comercio Electrónico

Secretaría General

Econ. Expidio Palacios
Secretario General

La Gestión del Riesgo incluye los siguientes procesos:

- Establecimiento del contexto: Se definen los objetivos, alcance y la organización para todo el proceso.
- Identificación de riesgos: Consiste en determinar qué puede provocar pérdidas en la organización.
- Estimación de riesgos: Utilizar métodos cuantitativos o cualitativos para obtener una cuantificación de los riesgos identificados, teniendo en cuenta los activos, amenazas y controles.
- Evaluación de riesgos: Se comparan los riesgos estimados con los criterios de evaluación y aceptación de riesgos definidos en el establecimiento del contexto
- Tratamiento de riesgos: Se define la estrategia para tratar cada uno de los riesgos valorados; reducir, aceptar, eliminar o transferir.
- Aceptación de riesgos: Se determinan los riesgos que se decide aceptar y su justificación correspondiente
- Comunicación de riesgos: Todos los grupos de interés intercambian información sobre los riesgos.
- Monitorización y revisión de riesgos: El análisis de riesgos se actualiza con todos los cambios internos o externos que afectan a la valoración de los riesgos.

El resultado debe ser un compromiso razonable entre los costos económicos y operacionales de las medidas de protección, y obtener mejoras en la capacidad de lograr la misión de la organización.

Se debe seguir un proceso similar al descrito en los documentos indicados en las referencias, para realizar el proceso de evaluación de riesgos.

El reporte de la valoración de los riesgos debe tener lineamientos dados en la siguiente estructura, un ejemplo se muestra en el Anexo N° 1.

MINISTERIO DE INDUSTRIA Y COMERCIO - Secretaría General - ES COPIA FIEL DEL ORIGINAL

Econ. Expidio Palacios
Secretario General

5.3.4.3 **Estándares de Evaluación**

- NP ISO/IEC 27001:2014
- ISO/IEC 27005:2011

Abog. Rodolfo Colón A. DIRECTOR GENERAL Firma Digital y Comercio Electrónico

5.3.4.4 **Documentación Solicitada**

- Copia del documento correspondiente a la Evaluación de Riesgos.

5.3.4.5. **Detalles de la Evaluación**

Aspectos	Evaluación
Reporte de la valoración de riesgos	Verificar que los riesgos considerados sean reales. Validar que riesgos relevantes no hayan sido omitidos. Verificar la valoración adecuada de los riesgos. Constatar si hay un plan de mantenimiento de la valoración.
Estructura del proceso de valoración de riesgos	Verificar si el proceso de valoración ha sido realizado o auditado por un ente calificado.

5.3.5. **Política de Seguridad de la Información (Documentación y mantenimiento)**

5.3.5.1 **Objetivo:** Comprobar a través de este documento que el PSC tiene claros los objetivos de seguridad relevantes para el negocio y que las instancias de gestión del PSC apoyan formalmente esta política.

5.3.5.2 **Descripción:** La política de seguridad es una declaración de objetivos de seguridad. Solo contiene objetivos de seguridad que son factibles de lograr a través de acciones, procedimientos y mecanismos implementados por el PSC. Si el PSC tiene en otra organización algún aspecto de seguridad o confianza, entonces debe indicarse claramente.

La política de seguridad debe cumplir al menos con los siguientes requerimientos:

a) Los objetivos de seguridad deben ser consecuencia de la Evaluación de Riesgos y Amenazas, de forma tal que los objetivos de la Política de seguridad y sus defensas asociadas correspondan al nivel de riesgo requerido para que un PSC sea una CA de confianza.
b) Debe estar basada en las recomendaciones del estándar NP ISO27002/2014 Anexo A Dominio 5, los cuales se transcriben en el Anexo N° 2 de este documento de evaluación.
c) Los objetivos de la política son de alto nivel y no técnicos, por tanto debe ser lo suficientemente general para permitir alternativas de implementación tecnológica.
d) Si la complejidad de los objetivos así lo requieren, la política puede estar conformada por más de un documento; esto es, puede haber una política general soportada por políticas específicas.
e) En esta política de seguridad deben estar incluidos los elementos contenidos en la CP y CPS.

Este documento debe identificar los objetivos de seguridad relevantes y las amenazas potenciales relacionadas a los servicios suministrados, así como las medidas tomadas para evitar o limitar los efectos de estas amenazas.

ES COPIA FIEL DEL ORIGINAL

Abog. Rodrigo Rolón A.
Dirección General
Firma Digital y Comercio Electrónico

Econ. Expidio Palacios
Secretario General

Adicionalmente, la documentación debe describir las reglas, directivas y procedimientos que indican como son provistos los servicios específicos y las medidas de seguridad asociadas.

En el Anexo N° 4 de este documento se describen los principales aspectos que una política de seguridad debe considerar.

Para los propósitos de la habilitación de un PSC, algunos de los aspectos más relevantes han sido incorporados en criterios separados para así facilitar el proceso de evaluación y donde estos se detallan completamente. Por ello, este documento puede expresar en forma general aquellos aspectos de la seguridad organizacional que se tratan en documentos específicos.

5.3.5.3 Estándares de Evaluación

- NP ISO/IEC 27001:2014
- ISO/IEC 27002:2013. Dominio 5: Política de Seguridad

5.3.5.4 Documentación Solicitada

Copia del documento correspondiente a la Política de seguridad de la organización.

5.3.5.5 Detalles de la Evaluación

Aspectos	Evaluación
Conformidad con el estándar ISO 27002 de acuerdo al control 5.1.1	Verificar que los requerimientos del control 5.1.1 descritos, están incorporados.
Conformidad con el estándar ISO 27002 de acuerdo al con control 5.1.2	Verificar que se ha incluido un procedimiento de revisión y evaluación periódica de la política de seguridad.
Conformidad con el estándar NP ISO/IEC 27001:2014 sección 5.2.	Verificar que los requerimientos de la sección 5.2. estén incorporados
Consistencia entre la política de seguridad y la CPS y CP	Constatar la consistencia de la política de seguridad con la CP y CPS.
Relación entre la Evaluación de Riesgos y la Política de seguridad	Verificar que los principales aspectos de la política de seguridad son coherentes con los niveles de riesgo determinados en la evaluación formal de riesgos conforme al Anexo N° 4.
Claridad de los objetivos de seguridad	Verificar que se establecen objetivos de seguridad claros relacionados con la protección de los procesos de negocios, activos y servicios del PSC.

5.3.6 Plan de Continuidad del Negocio y Recuperación ante Desastres

5.3.6.1 **Objetivo:** Comprobar que el PSC tiene planes establecidos para disminuir a un nivel aceptable el efecto de interrupciones del servicio del PSC, mediante una combinación de controles preventivos y planes de contingencia.

ESCORIA FIEL DEL ORIGINAL

Abog. Nadys Rolón A. DIRECTORA GENERAL Firma Digital y Comercio Electrónico

Econ. Expidio Palacios Secretario General

5.3.6.2 **Descripción**

El Plan de Continuidad del Negocio y de Recuperación de Desastres, debe describir cómo los servicios serán restaurados ante un evento de desastre, una caída de los sistemas o fallas de seguridad.

Dicho plan debe ser mantenido y probado periódicamente y debiera ser parte integral de los procesos de la organización.

En general, para lograr la implantación de proceso de Gestión de Continuidad de negocios se debe alinear con la ISO 22301:2012 que establece dicho proceso.

En particular, el documento describe la prioridad de restauración para asegurar la continuidad de los negocios de terceros que sean dependientes de la operación del PSC.

Este documento debe ceñirse a los lineamientos brindados por la NP-ISO/IEC 27001:2014. Anexo A. Dominio 17.

Este documento también debe describir los procedimientos de emergencia a ser seguidos en al menos los siguientes escenarios:

- Desastre que afecte el funcionamiento de los productos de software en el cual el PSC basa sus servicios.
- Incidente o posible incidente de seguridad que afecte la operación del sistema en el cual el PSC basa sus servicios.
- Compromiso de la clave privada de firma del PSC.
- Falla de los mecanismos de Auditoría.
- Falla en el hardware donde se ejecuta el producto en el cual el PSC basa sus servicios, este debe incluir los servidores, dispositivos criptográficos, dispositivos de seguridad y dispositivos de comunicaciones.

Se debieran identificar los eventos que pueden causar interrupciones a los procesos comerciales y operacionales, junto con la probabilidad y el impacto de dichas interrupciones y sus consecuencias para la seguridad de la información, esto según la NP-ISO/IEC 27001:2014.

El plan debe además incluir mecanismos para la preservación de evidencia de mal uso de los sistemas, cuyo propósito es proporcionar evidencia admisible en una autoridad jurisdiccional en alguna fecha posterior.

Econ. Expidio Palacios
Secretario General

5.3.6.3 **Estándares de Evaluación**

- NP-ISO/IEC 27001:2014. Anexo A. Dominio 17
- ISO/IEC 27002:2013. Dominio 17
- ISO 22301:2012

5.3.6.4 **Documentación solicitada**

- Documento correspondiente al Plan de Continuidad del Negocio y Recuperación ante Desastres.
- Documento de Evaluación de Riesgo.

5.3.6.5 **Detalles de la Evaluación**

Aspectos	Evaluación
Conformidad con el estándar ISO 27002 controles 17.1.1 al 17.1.2	Verificar que los requerimientos del dominio 17 indicados en el Anexo N° 2, están incorporados.
Conformidad con el estándar ISO 27002:2013control 17.1.3	Comprobar que se ha incluido un procedimiento de verificación, revisión y evaluación periódica de la política de seguridad.
Conformidad con el estándar ISO 27002:2013 control 17.2.1	Comprobar la disponibilidad de instalaciones para el procesamiento de la información.
Relación entre la Evaluación de Riesgos y el Plan de Continuidad del Negocio (BCP) y Plan de Recuperación de Desastres (DRP)	Verificar que los principales aspectos de los planes son coherentes con los niveles de riesgo determinados en una evaluación formal de riesgos.
Viabilidad de las facilidades computacionales alternativas	Chequear que las facilidades computacionales alternativas consideradas en el plan, cumplen con los requerimientos mínimos para la operación del PSC.
Elementos de Auditoría	Verificar que el sistema en el cual el PSC basa sus servicios provee mecanismos de preservación de los elementos de Auditoría.

5.3.7 **Plan de un Sistema de Gestión de Seguridad de la Información**

5.3.7.1 **Objetivo:** Comprobar a través de este documento que el PSC tiene un Plan de Seguridad coherente con su Política de Seguridad, que permita mostrar un nivel de confianza consistente con los objetivos del negocio.

5.3.7.2 **Descripción**

El Plan de un Sistema de Gestión de Seguridad de la información tiene como propósito describir los requerimientos de seguridad de la información y los controles desplegados o planificados para satisfacer dichos requerimientos. Adicionalmente, debe delinear las responsabilidades y conductas esperadas de los individuos que acceden a los sistemas.

Por lo tanto, el Plan de Seguridad de Sistemas debe describir las acciones operacionales, procedimientos y mecanismos que permitan lograrlos objetivos indicados en la Política de Seguridad del PSC, posteriormente esto debe permitir cumplir con un Sistema de Gestión de Seguridad de la Información como lo establece la NP ISO 27001/2014.

El Plan de Seguridad debe considerar al menos los dominios 5 al 18 del estándar ISO 27002:2013. Sin embargo, en este requisito se evalúan en particular los siguientes aspectos:

- Aspectos Organizativos de la Seguridad de la Información.
- Gestión de Activos.
- Control del Acceso.
- Cifrado.
- Seguridad en la operativa.
- Seguridad en las Telecomunicaciones.

En el anexo N° 5 se mencionan otros elementos a considerar para la evaluación del plan de seguridad de la información.

Se considera que este Plan es una declaración de intenciones del PSC, por lo que la evaluación bajo este requisito no es una certificación de su nivel de seguridad. El proceso de evaluación bajo este requisito indica el nivel de confiabilidad del PCS si este cumple con el plan de seguridad de la información.

5.3.7.3 **Estándares de Evaluación**

- NP ISO/IEC 27001:2014
  ISO/IEC 27002:2013

5.3.7.4 **Documentación Solicitada**

- Copia del documento correspondiente al Plan de Seguridad de Información.

Econ. Expidio Palacios
Secretario General

5.3.7.5 Detalles de la Evaluación

Aspectos	Evaluación
Relación entre el Plan de Seguridad y los recursos asignados	Verificar que el PSC puede justificar la disponibilidad de los recursos y capacidades para implementar los mecanismos y los recursos asignados a procedimientos de seguridad.
Relación entre el Plan de Seguridad y Evaluación de Riesgos	Comprobar que los procedimientos y mecanismos de seguridad permiten lograr el riesgo residual determinado en la Evaluación de Riesgos.
Relación entre Plan de Seguridad y Política de Seguridad	Confirmar que los procedimientos y mecanismos de seguridad permiten lograr los objetivos de la Política de Seguridad.
Mantenimiento del Plan de seguridad	Verificar que el Plan de Seguridad incluye los procedimientos que garanticen que la seguridad del PSC se mantiene en el tiempo ante cambios en: amenazas, personal, servicios, componentes tecnológicos, etc.
Relación del Plan de Seguridad con la CP y CPS	Verificar que los objetivos de seguridad enunciados en la CP y CPS del PSC se logran a través del Plan de Seguridad.
Requerimientos ISO27002:2013, dominio 6	Confirmar que los controles de "Los aspectos organizativos de la seguridad de la información" del estándar ISO 27002:2013 están considerados.
Requerimientos ISO27002:2013, dominio 8	Verificar que se han tomado en cuenta los controles de "Gestión de activos" del estándar ISO 27002:2013.
Requerimientos ISO27002:2013, dominio 9	Verificar la inclusión de los controles de la cláusula de "Control de acceso" del estándar ISO 27002:2013.
Requerimientos ISO 27002:2013, dominio 10	Verificar que el Plan de Seguridad contiene un Plan de Administración de Claves Criptográficas para todo el ciclo de vida de estas claves.
Requerimientos ISO27002:2013, dominio 12	Verificar que los controles de "Seguridad en la operativa" del estándar ISO 27002:2013 están considerados.
Requerimientos ISO27002:20, dominio 13	Verificar que los controles de "Seguridad en las telecomunicaciones" del estándar ISO 27002:2013 están considerados.
Protección del repositorio de acceso público	Verificar que el Plan de Seguridad contiene medidas especiales de protección del repositorio público de certificados.
Protección de información privada	Asegurarse de que el plan incluye medidas de protección de información privada recaudada durante el proceso de registro.

5.3.8 Implementación del Plan del Sistema de Gestión de Seguridad de la Información

5.3.8.1 Objetivo

Comprobar que el PSC tiene implementado un Plan de Seguridad coherente con su Política de Seguridad, que permita mostrar un nivel de confianza consistente con los objetivos del negocio.

5.3.8.2 Descripción

El PSC debe mostrar que sus procedimientos de administración de seguridad y la capacidad de disponer de las instalaciones, están conforme al Plan de Seguridad.

Se evalúan:

- Acciones operacionales, procedimientos y mecanismos que permiten lograr los objetivos indicados en el Plan de Seguridad del PSC.

- Controles desplegados o planificados para satisfacer dichos requerimientos.
- Que estos controles sean coherentes con los requerimientos del estándar ISO 27002:2013. En particular los planes correspondientes a los siguientes aspectos:
    - Aspectos Organizativos de la Seguridad de la Información.
    - Gestión de Activos.
    - Control del Acceso.
    - Cifrado.
    - Seguridad en la operativa.
    - Seguridad en las Telecomunicaciones.

La evaluación combinará entrevistas con el personal del PSC y Auditorías que incluirán visitas a las instalaciones del PSC para verificar la implementación práctica del plan.

5.3.8.3 **Estándares de Evaluación**

- NP ISO/IEC 27001:2014
- ISO/IEC 27002:2013

5.3.8.4 **Documentación Solicitada**

Documento descriptivo de la implementación del Plan de Seguridad de la información del solicitante a constituirse en PSC, el cual será validado al momento de la auditoría.

5.3.8.5 **Detalles de la Evaluación**

Aspectos	Evaluación
Relación entre el Plan de Seguridad y los recursos asignados	Verificar que el PSC dispone de los recursos y capacidades para implementar los mecanismos y procedimientos de seguridad.
Relación entre el plan de seguridad y política de seguridad	Comprobar que los procedimientos y mecanismos de seguridad implementados permiten lograr los objetivos de la política de seguridad.
Relación entre Plan de Seguridad y Evaluación de Riesgos	Verificar que los procedimientos y mecanismos de seguridad implementados permiten lograr el riesgo residual determinado en la Evaluación de Riesgos.
Mantenimiento del Plan de Seguridad	Confirmar que la implementación del Plan de Seguridad incluye los procedimientos que garanticen que la seguridad del PSC se mantiene en el tiempo ante cambios en: amenazas, personal, servicios, componentes tecnológicos, etc.
Relación del Plan de Seguridad con prácticas y la Política de Certificados	Verificar que los objetivos de seguridad enunciados en la CP y CPS del PSC se logran a través del Plan de Seguridad.
Requerimientos ISO27002:2013, dominio 6	Verificar que los controles de "Aspectos organizativos de la Seguridad de la información" recomendados por el estándar ISO 27002:2013 están implementados.
Requerimientos ISO27002:2013, dominio 8	Comprobar que los controles de "Gestión de activos" recomendados por el estándar ISO 27002:2013 están implementados.

Requerimientos SO27002:2013, dominio 9	Verificar la implantación de los controles de la cláusula de "Control del acceso" recomendados por el estándar ISO 27002:2013.
Requerimientos ISO27002:2013, dominio 10	Verificar que estén implementados los controles de "Cifrado" del estándar ISO 27002:2013.
Requerimientos ISO27002:2013, dominio 12	Validar que los controles de "Seguridad de la operativa" recomendados por el estándar ISO 27002:2013 estén implementados.
Requerimientos ISO27002:2013, dominio 13	Validar que los controles de "Seguridad de las telecomunicaciones" recomendados por el estándar ISO 27002:2013 estén implementados.
Protección del repositorio de acceso público	Verificar que la implementación del Plan de Seguridad contiene medidas especiales de protección del repositorio Público del PSC.
Protección de información privada	Comprobar que en la implementación del plan se protegió la información privada recolectada durante el proceso de registro.

5.3.9 **Plan de Administración de Claves Criptográficas. (Implementación y Mantenimiento)**

5.3.9.1 **Objetivo:** Comprobar que el PSC implementa un plan de administración del ciclo de vida de sus claves criptográficas coherente con su política de seguridad, que permita mostrar un nivel de confianza consistente con los objetivos del negocio.

5.3.9.2 **Descripción:** Las claves criptográficas son la base de una infraestructura de clave pública (PKI), siendo el elemento principal a resguardar y administrar por el PSC, y por lo tanto requiere de un plan específico para su administración.

Contenido de este plan:

- ✓ Documentación del ciclo de vida completo de las claves criptográficas, esto es:
- Generación de las claves del PSC (Autoridad de Certificación).
- Almacenamiento, respaldo y recuperación de la clave privada de la CA.
- Distribución de la clave pública de la CA.
- Uso de la clave privada por parte de la CA.
- Término del ciclo de vida de la CA.
- Administración del ciclo de vida del hardware criptográfico utilizado por la CA.
- Servicios de administración de las claves de los suscriptores suministradas por la CA (generación de clave).
- Preparación de los dispositivos seguros de los suscriptores.
- A su vez el plan debe ser consistente con la CP y la CPS.

Abog. Rubys Rolón A. DIRECTOR GENERAL Firma Digital y Comercio Electrónico

ESTA COPIA ES FIEL DEL ORIGINAL - MIC - Secretaría General

Econ. Expidio Palacios
Secretario General

5.3.9.3 **Estándares de Evaluación**

- FIPS PUB 140-2
- ETSI TS 102 042

5.3.9.4 **Documentación Solicitada**

- Documento descriptivo de la implementación del Plan de Administración de Claves Criptográficas de la Organización.

5.3.9.5 **Detalles de la Evaluación**

Aspectos	Evaluación
Relación entre el Plan de Administración de Claves y los recursos asignados	Verificar que el PSC dispone de los recursos y capacidades adecuados para implementar el plan de administración de claves.
Relación entre el Plan de Administración de Claves y Evaluación de Riesgos	Verificar que los procedimientos y mecanismos de administración de claves implementados permiten lograr el riesgo residual determinado en la Evaluación de Riesgos.
Mantenimiento del Plan de Administración de Claves	Confirmar que los procedimientos implementados de acuerdo al Plan de Administración de Claves posibilitan que la seguridad de las claves se mantiene en el tiempo ante cambios en: amenazas, personal, servicios, componentes tecnológicos, etc.
Relación del Plan de Administración de Claves con la CP y CPS	Comprobar que los objetivos de seguridad enunciados en la CP y CPS del PSC se logran a través de la implementación del Plan de Administración de Claves.
Generación de Claves de Autoridad de Certificación	Verificar que los requerimientos de Generación de Claves de la CA son los adecuados y requeridos por la normativa y reglamentaciones.
Almacenamiento, Respaldo y Recuperación de Claves de Autoridad de Certificación	Verificar que los requerimientos de Almacenamiento, Respaldo y Recuperación, están considerados.
Distribución de clave pública de Autoridad de certificación	Confirmar que los requerimientos de distribución de la clave pública de la CA, están considerados.
Uso de claves de Autoridad de certificación	Verificar que los requerimientos de uso de clave de la CA, están considerados.
Fin del ciclo de vida de la Clave de la Autoridad de Certificación	Comprobar que los requerimientos de fin del Ciclo de Vida de la Clave de la CA, están considerados.
Gestión del ciclo de vida del hardware criptográfico utilizado para firmar los certificados	Verificar que los requerimientos de Administración del hardware criptográfico están considerados.

Nivel de seguridad del dispositivo seguro del PSC	Verificar que el dispositivo seguro de los PSC cumple como mínimo con los requerimientos del estándar FIPS PUB 140-2 nivel 3 (overall) en sus elementos de seguridad e implementación de los algoritmos criptográficos estándares.
Nivel de seguridad de dispositivo seguro de los suscriptores	Verificar que el dispositivo seguro de los suscriptores cumple como mínimo con los requerimientos del estándar FIPS PUB 140-2 nivel 2 (overall) para personas físicas y nivel 3 (overall) para persona jurídica en sus elementos de seguridad e implementación de los algoritmos criptográficos estándares.

5.3.10 Evaluación de la Plataforma Tecnológica

5.3.10.1 **Objetivo:** Evaluar los elementos de seguridad de la plataforma tecnológica utilizada para la generación, publicación y administración de certificados digitales y CRL.

5.3.10.2 **Descripción:** Evaluar la seguridad de los elementos que constituyen la plataforma tecnológica del PSC. Se debe considerar componentes hardware y software que conforman la infraestructura PKI del PSC, así como, todos los elementos de apoyo a su operación e interrelación, como protocolos y servicios.

Los elementos a considerar son:

- Módulo criptográfico.
- Módulo CA (Autoridad de Certificación).
- Módulo RA (Autoridad de Registro).
- Módulo de Almacenamiento y Publicación de Certificados.
- Protocolos de comunicación entre CA y RA.
- Elementos de administración de logs y Auditoría.
- Arquitectura de la red.

5.3.10.3 Estándares de Evaluación

- FIPS PUB 140-2

5.3.10.4 Documentación Solicitada

- Documento descriptivo de la implementación de la infraestructura tecnológica. Este documento debe incluir al menos, planos de interconexión de sistemas, cableado de red de datos, cableado de fuente de alimentación de energía eléctrica (principal y auxiliar), dispositivos de seguridad y control de acceso, y todo aquello relevante que permita demostrar la confiabilidad de la infraestructura tecnológica.

ES COPIA FIEL DEL ORIGINAL

Abog. Rolón A. Director General Firma Digital y Comercio Electrónico

Econ. Expidio Palacios
Secretario General

- Manuales del fabricante de los productos hardware y software relevantes. Documentación del fabricante que acredite el correspondiente nivel de seguridad.
- Manuales descriptivos del diseño físico y lógico de la red. Con detalle de servicios implementados.

5.3.10.5 **Detalles de la Evaluación**

Aspectos	Evaluación
Módulo criptográfico	1. Funcionalidad y operación: Generar pares de clave privada y pública con claves de al menos 4096 bits. Capacidad de firma y cifrado 2. Seguridad Existencia de sistema de control de acceso para acceder a la clave privada. Existencia de controles de acceso para acceder a funcionalidades de firma y cifrado. 3. Ciclo de vida Capacidad de respaldar la clave privada, en forma segura. Capacidad de recuperar la clave privada de Respaldo (backup). 4. Auditoría Capacidad de generar log auditable para administración de contingencia y accesos maliciosos. 5. Documentación Manuales de operación, configuración y puesta en marcha. Procedimiento de recuperación ante contingencia.
Módulo CA (Autoridad de Certificación)	1. Funcionalidad y operación: Capacidad para generar certificados con claves de al menos 4096. Capacidad de revocación de certificados Capacidad para generar CRLs. Indicar fecha de publicación y de nueva renovación de la CRL. Capacidad para generar certificados de según el tipo solicitado. Capacidad de generar certificados de comunicación segura, entre CA y RA, si corresponde a la arquitectura. Capacidad de entregar certificados y CRL a directorios públicos X500. 2. Seguridad. Existencia de sistema control de acceso para acceder a la generación de certificados. Existencia de sistema de control de acceso para acceder a los sistemas de administración y Auditoría. 3. Ciclo de vida. Capacidad de emitir y revocar certificados. 4. Auditoría. Capacidad de generar log auditable para administración de contingencia. Actividades del personal autorizado y accesos maliciosos. 5. Documentación. Manuales de operación, configuración y puesta en marcha. Procedimiento de Recuperación ante contingencia.

Módulo de RA (Autoridad de Registro)	1. Funcionalidad y operación: Capacidad de recibir requerimientos de certificados. Solicitar certificado a la CA. 2. Seguridad: Existencia de sistema control de acceso para acceder a la generación de certificados. Existencia de sistema de control de acceso para acceder a los sistemas de administración y Auditoría. 3. Ciclo de vida: Capacidad de validación de datos de los certificados y solicitud de certificados a la CA. 4. Auditoría: Capacidad de generar log auditable para administración de contingencia y accesos maliciosos. 5. Documentación: Manuales de operación, configuración y puesta en marcha. Procedimiento de Recuperación ante contingencia.
Módulo de Almacenamiento y Publicación de Certificados	Almacenamiento de certificados en base de datos X500, y publicación a través de protocolos OCSP V1.0.
Protocolos de comunicación entre RA y CA	Capacidad de generar certificados de comunicación segura, entre CA y RA, si corresponde a la arquitectura, utilizando un protocolo estándar de la industria.
Elementos de administración de log y Auditoría	Deben existir módulos de log y de Auditoría, que permitan verificar los intentos de acceso, los accesos y las operaciones dañinas, sean estas intencionadas o no. El PSC debe contar con un sistema centralizado de logs (Syslog Server), que permita almacenar todos los eventos de los sistemas críticos y/o componentes de red y que puedan ser administrados especialmente en cuanto a envío de alertas de eventos bien específicos.
Arquitectura de Red	Se verificará que en diseño e implementación de la red se hayan considerado los requisitos técnicos y de seguridad.

5.3.11 **Declaración de Prácticas de Certificación (CPS) y Política de Certificados (CP)**

5.3.11.1 **Objetivo:** Verificar que el PSC disponga de un documento, que señale los procedimientos de gestión de certificados y los diferentes tipos de certificados a otorgar, según lo establecido en:

- La Ley N° 4017/10"De Validez Jurídica de la Firma Electrónica, La Firma Digital, Los Mensajes de Datos y El Expediente Electrónico".
- Ley N° 4610/12 que la modifica parcialmente y amplía.
- El Decreto N° 7369/11 y las Reglamentaciones emitidas por el Ministerio de Industria y Comercio (MIC) en su calidad de Autoridad de Aplicación.

5.3.11.2 **Descripción:** Los elementos principales que debe contener la CPS, son las delimitaciones de responsabilidad y las obligaciones tanto del PSC, como del suscriptor.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Econ. Expidio Palacios
Secretario General

Además debe quedar explícito, tanto el ciclo de vida de los certificados, desde su solicitud hasta el término de su vida útil, como el ciclo de vida del PSC, desde el inicio hasta el fin del mismo.

Este requisito es relevante no sólo para el suscriptor del certificado sino para todas las entidades involucradas, incluyendo quienes reciben un documento firmado electrónicamente.

En la CP y CPS se verificarán al menos: que permita la interoperabilidad con otro PSC y entregue la confianza necesaria para que los documentos firmados en forma electrónica por el suscriptor de un certificado, se ciñan a la forma de operar recomendada y sean equivalentes a una firma manuscrita en las circunstancias que indica la Ley N° 4017/10.

5.3.11.3 **Estándares de Evaluación**

- RFC 3647
- ETSI TS 102 042

5.3.11.4 **Documentación Solicitada:** Documento de la Declaración de Prácticas de Certificación (CPS) y Política de Certificados (CP) con los diferentes tipos de estructura de campos de certificados. Ver Anexo N° 3.

5.3.11.5 **Detalles de la Evaluación**

Aspectos	Evaluación
Verificar estructura	Verificar que la CPS y CP contienen al menos los tópicos indicados en el Anexo No 3 de este documento.
Suscriptor	Se debe indicar a quien se le puede otorgar un certificado digital.
Usos del certificado	Se debe indicar los propósitos para el cual fue emitido el certificado y sus limitaciones, indicando cuales usos son permitidos y cuáles no.
Publicación de información de la CA y Repositorios de los Certificados	Se debe verificar la publicación de los certificados, CPS, CP y CRL, su frecuencia de publicación, así como la disponibilidad de los repositorios y sus controles de acceso.
Identificación y Autenticación	Se debe comprobar el registro del nombre del suscriptor, la validación inicial de su identidad, así como la identificación y autenticación de las solicitudes de revocación del certificado.
Ciclo de vida de los certificados	Confirmar que para cada etapa del ciclo de vida de los certificados (emisión/revocación) estén establecidos los procedimientos y deberes del PSC.
Controles de seguridad física, de gestión y de operaciones	Se debe comprobar la existencia de los controles de seguridad física, funcionales, de seguridad personal, los procedimientos de control de seguridad, los archivos de informaciones y registros. Además se debe contemplar que exista la documentación de procedimientos de la recuperación en caso de desastre y en caso del cese de la actividad del PSC, que incluyan los procedimientos de término y de traspaso a otro PSC u organismo que asuma la responsabilidad de mantener la continuidad de los servicios, en tanto existan. certificados vigentes.

Aspectos	Evaluación
Controles de Seguridad técnica	Comprobar la existencia de las medidas de seguridad adoptadas por el PSC para la generación e instalación de las claves privada y pública, la protección de la clave privada, los datos de activación. Además se debe verificar los siguientes controles de seguridad: del computador, del ciclo de vida y de la red, así como los controles de ingeniería de los módulos criptográficos.
Perfiles de certificados, OCSP y CRL	Se verificará que el perfil de los certificados cumpla con los estándares internacionales vigentes, aplicables para las infraestructuras de claves públicas y los certificados digitales. En forma similar se verificará que el perfil de la CRL y el OCSP se adapten al estándar correspondiente.
Auditoría de conformidad	Se debe verificar que el PSC cumpla con la frecuencia de la realización de auditorías internas.
Aranceles y responsabilidad financiera	Se refiere a las tasas establecidas para la gestión de certificados.
Confidencialidad de la información de los Suscriptores/protección de datos	Existencia de procedimientos de protección de la información de los suscriptores.
Obligaciones CA, RA, suscriptor	Descripción de las obligaciones que contraen las entidades involucradas en la emisión y utilización de un certificado.
Las obligaciones y responsabilidades del PSC	Comprobar que exista una declaración de las obligaciones y deberes del PSC.
Las obligaciones y responsabilidades del suscriptor	Verificar que existan definiciones de los deberes y obligaciones de los suscriptores.
Renuncias de garantías y limitación de responsabilidades	Concordancia de la CP y CPS con los procedimientos operacionales.
Modificaciones	Entre los requisitos comerciales y legales, todo PSC debe tener procedimientos que especifiquen una autoridad que apruebe los cambios aplicables a su CP y CPS, así como su publicación y notificación.

5.3.12 Modelo de Operación de la Autoridad de Certificación (CA) del PSC

5.3.12.1 **Objetivo:** Comprobar a través de la documentación presentada que el Modelo de Operación cumple con los requerimientos y obligaciones que dispone la Ley N° 4017/10 "De Validez Jurídica de la Firma Electrónica, La Firma Digital, Los Mensajes de Datos y El Expediente Electrónico", Ley N° 4610/12 que la modifica parcialmente y amplía, el Decreto N° 7369/11 y las Reglamentaciones emitidas por el Ministerio de Industria y Comercio (MIC) en su calidad de Autoridad de Aplicación, en relación con la confiabilidad e interoperabilidad en la forma de operar y prestar los servicios de la CA en un PSC.

ES COPIA FIEL DEL ORIGINAL

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

MINISTERIO DE INDUSTRIA Y COMERCIO - Secretaría General -

Econ. Expidio Palacios
Secretario General

5.3.12.2 **Descripción**

El Modelo de Operación debe responder al menos a las siguientes preguntas:

- ¿Cuáles son los servicios prestados por la CA del PSC?
- ¿Cómo se interrelacionan los diferentes servicios?
- ¿En qué lugares opera?
- ¿Qué tipos de certificados se entregan?
- ¿Cómo se pretende hacer esto, incluyendo servicios con terceros?
- ¿Cómo se protegerán los activos?

5.3.12.3 **Estándares de Evaluación**

- No aplica

5.3.12.4 **Documentación Solicitada**

- Descripción del Modelo de Operación de la CA del PSC.

5.3.12.5 **Detalles de la Evaluación**

Aspectos	Evaluación
Consistencia del documento	Se verificará que el documento incluya todas las partes mencionadas en el documento tipo descrito en el Anexo N° 7.
Resumen Ejecutivo	Se verificará que el resumen incluya: a) Un resumen coherente del contenido del documento. b) La historia de la empresa. c) Relaciones comerciales con proveedores de insumos o servicios para sus operaciones.
Componentes del Sistema	Se verificará que el modelo comprenda los siguientes aspectos: a) Interfaces con RA. b) Implementación de elementos de seguridad. c) Procesos de administración. d) Sistema de directorios para los certificados. e) Procesos de Auditoría y respaldo. f) Bases de Datos. g) Privacidad. h) Entrenamiento del persona
Proceso de Certificación	Se verificará que el modelo considere la generación de claves para el suscriptor de acuerdo a la CP.
Plan de Auditoría	Se verificará que el modelo considere en el plan de Auditoría lo siguiente: a) Seguridad y dispositivos de seguridad b) Restricciones del personal c) Interfaces de administración d) Procedimientos de recuperación de desastres e) Procedimientos de respaldo

Aspectos	Evaluación
Seguridad	Se verificará que el modelo incluya los requerimientos de: a) La seguridad física y ambiental de las instalaciones. b) Seguridad de recursos humanos. c) Nivel de seguridad del módulo criptográfico.

5.3.13 **Modelo de Operación de la Autoridad de Registro (RA) del PSC**

5.3.13.1 **Objetivo:** Comprobar los aspectos mínimos que disponen la Ley N° 4017/10 "De Validez Jurídica de la Firma Electrónica, La Firma Digital, Los Mensajes de Datos y El Expediente Electrónico", Ley N° 4610/12 que la modifica parcialmente y amplía, el Decreto N° 7369/11 y las Reglamentaciones emitidas por el Ministerio de Industria y Comercio (MIC) en su calidad de Autoridad de Aplicación, con relación a conformidad con los requisitos de confiabilidad e interoperabilidad en la forma de operar y prestar sus servicios.

5.3.13.2 **Descripción**

El Modelo de Operación debe responder a:

- ¿Cuáles son los servicios de registro prestados por el PSC?
- ¿En qué lugares se ofrece dichos servicios?
- ¿Qué tipos de certificados se entregan?
- ¿Cómo se pretende hacer esto, incluyendo los servicios prestados por terceros?

Según la norma técnica ETSI TS 102 042 se entiende que el PSC tiene la obligación de generar y entregar en forma segura la clave privada del suscriptor de un certificado de firma electrónica emitido por él, asegurar la fiabilidad del dispositivo seguro y de los mecanismos que el suscriptor utiliza para firmar.

5.3.13.3 **Estándares de Evaluación**

- ETSI TS 102 042

5.3.13.4 **Documentación Solicitada**

- Descripción del Modelo de Operación de la RA

Abog. Rubys Rolón A. DIRECTORA GENERAL Firma Digital y Comercio Electrónico

ES COPIA FIEL DEL ORIGINAL - MINISTERIO DE INDUSTRIA Y COMERCIO - Secretaría General

Econ. Expidio Palacios
Secretario General

5.3.13.5 **Detalles de la Evaluación**

Aspectos	Evaluación
Consistencia del documento	Se verificará que el documento incluya todas las partes requeridas del documento tipo descrito en el Anexo N° 8 de éste documento.
Resumen ejecutivo	Se valida que el resumen ejecutivo sea coherente con el contenido del documento.
Componentes del sistema	Se verificará que el modelo comprenda los siguientes aspectos: a) Interfaces con la CA b) Implementación de dispositivos de seguridad c) Procesos de administración d) Procesos de Auditoría y respaldo e) Bases de Datos f) Privacidad g) Entrenamiento del personal
Proceso de Certificación	Se valida que el modelo de registro del suscriptor provea una identificación unívoca del mismo y el modelo de uso de la clave privada provea la confianza requerida en el sistema.
Plan de auditoría	Se verificará que el modelo de la RA incluya auditoría de lo siguiente: a) Dispositivos de seguridad b) Seguridad c) Restricciones del personal d) Interfaces de administración e) Procedimientos de recuperación de desastres f) Procedimientos de respaldo
Seguridad	Se verificará que el modelo de la RA incluya lo siguiente: a) Descripción de la seguridad física y ambiental de las instalaciones b) Seguridad de recursos humanos

5.3.14 **Manual de Operación de la Autoridad de Certificación (CA)**

5.3.14.1 **Objetivo:** Comprobar a través de la documentación presentada, el cumplimiento de los aspectos operacionales mínimos que dispone la Ley N° 4017/10 "De Validez Jurídica de la Firma Electrónica, La Firma Digital, Los Mensajes de Datos y El Expediente Electrónico", Ley N° 4610/12 que la modifica parcialmente y amplía, el Decreto N° 7369/11 y las Reglamentaciones emitidas por el Ministerio de Industria y Comercio (MIC) en su calidad de Autoridad de Aplicación, con relación a los requisitos de confiabilidad e interoperabilidad en la forma de manejar y prestar los servicios de la CA de un PSC.

5.3.14.2 **Descripción:** El propósito del manual es describir la administración diaria y las prácticas operacionales de la CA y garantizar que las directrices primarias de la CP y CPS estén implementadas operacionalmente; con el fin de facilitar al personal (de operaciones, consultores y/o auditores), la comprensión de esta información, se permite el uso de gráficos, diagramas de flujo, funcionales, líneas de tiempo, etc.

Abog. Aldys Rolón A.
Dirección General
Firma Digital y Comercio Electrónico

MINISTERIO DE INDUSTRIA Y COMERCIO
Secretaría General

Econ. Expidio Palacios
Secretario General

El Manual de Operación de la CA deberá tener al menos las siguientes características:

- Ser consistente con la Política de Certificados.
- Incluir la interacción entra la CA y la RA.
- Describir los controles de seguridad física, de red, de recursos humanos y de procedimientos.
- Incluir los procedimientos adoptados para el manejo de claves públicas y privadas.

5.3.14.3 **Estándares de Evaluación**

- ETSI TS 102 042
- RFC 3647

5.3.14.4 **Documentación Solicitada**

- Manual de operación de la CA del PSC

5.3.14.5 **Detalles de la Evaluación**

Aspectos	Evaluación
Nómina y descripción de cargos	Nómina de los cargos de personal, con la descripción de las responsabilidades y los procedimientos en que el personal realiza sus funciones.
Referencias de los cargos en los planes del PSC	Referencia del personal en los planes de continuidad del negocio y los planes de recuperación de desastres y emergencia.
Descripción de las Operaciones	Descripción detallada de los siguientes procedimientos: 1. Generación de pares de claves 2. Publicación de la CRL 3. Publicación de la información del certificado 4. Distribución de claves y certificados 5. Revocación de certificados 6. Medidas de control de acceso 7. Procedimientos de respaldo y recuperación
Actualización de CP y CPS	Procedimiento de actualización de la CP y CPS
Servicios de la CA	Descripción de los servicios de la CA
Interacción CA y la RA	El documento cubre la interacción entre la CA y RA

5.3.15 **Manual de Operación de la Autoridad de Registro (RA)**

5.3.15.1 **Objetivo:** Comprobar a través de la documentación presentada los aspectos operacionales mínimos que dispone la Ley N° 4017/10 "De Validez Jurídica de la Firma Electrónica, La Firma Digital, Los Mensajes de Datos y El Expediente Electrónico", Ley N° 4610/12 que la modifica parcialmente y amplía, el Decreto N° 7369/11 y las Reglamentaciones emitidas por el Ministerio de Industria y Comercio (MIC) en su calidad de Autoridad de Aplicación, con relación a los requisitos de confiabilidad e interoperabilidad del manejo del PSC para realizar las funciones de Autoridad de Registro.

5.3.15.2 **Descripción:** El Manual de Operación deberá describir como operará el servicio de registro del PSC y su administración diaria. Entre otros aspectos debería tenerlas siguientes características:

- Ser consistente con la CP.
- Describir el plan de entrenamiento de los empleados.
- Incluir la forma en que se verifica la identidad de las personas.
- Incluir procedimientos de entrega y uso de la clave privada por los suscriptores de los certificados. Según la norma ETSI TS 102 042, se entiende que el PSC tiene la obligación de generar y entregar en forma segura la clave privada del suscriptor de un certificado digital emitido por él, asegurar la fiabilidad del dispositivo seguro y los mecanismos que el suscriptor utiliza para firmar.

Contener la metodología adoptada para manejar los temas de:

- Análisis de riesgos.
- Plan de recuperación de desastres.
- Plan de seguridad.
- Incluir la interacción entre las unidades internas que cumplen la función de CA y RA.

5.3.15.3 **Estándares de Evaluación**

- RFC 3647
- ETSI TS 102 042

5.3.15.4 **Documentación Solicitada**

- Manual de Operación de la RA.
- Manual técnico de los dispositivos seguros de firma electrónica.

5.3.15.5 **Detalles de la Evaluación**

Aspectos	Evaluación
Nómina y descripción de cargos	Nómina de los cargos de personal empleado, con la descripción de los procedimientos operacionales y la forma en que los empleados realizan sus funciones.
Proceso de registro	Se verifica el registro del suscriptor. La autenticación, confirmación de su identidad y forma de política para comprobar el nombre del suscriptor.
Entrega segura de los datos de creación de firma	El PSC debe tener implementados procedimientos y prácticas que permitan entregar en forma personal y segura los datos de creación de firma al suscriptor del certificado.

Econ. Expidio Palacios
Secretario General

Dispositivo seguro y mecanismos de firma del suscriptor	El PSC debe tener implementados procedimientos y prácticas que aseguren que una vez entregados los datos de creación de firma sólo el suscriptor tenga control de ellos. El dispositivo seguro entregado al suscriptor debe firmar internamente el documento sin ser jamás accesible la clave privada del suscriptor. El mecanismo de control de acceso a la clave privada sólo debe ser conocido por el suscriptor al momento de la entrega del dispositivo y en lo posible modificable por el mismo suscriptor, antes de ser utilizado por primera vez. El dispositivo seguro debe contar con mecanismos que inhabiliten el dispositivo en caso de reiterados intentos fallidos de acceso. El PSC debe entregar al suscriptor herramientas, aplicaciones e instrucciones para que pueda firmar en forma segura.
Capacitación y servicio al suscriptor	El PSC debe implementar procedimientos de capacitación que permitan al suscriptor manejar en forma segura e informada el dispositivo de firma, y además mantener un servicio de atención para responder y solucionar dudas de los suscriptores.
Referencias de los cargos en los planes de continuidad de negocios del PSC	Referencia del personal en los planes de continuidad del negocio y los planes de recuperación de desastres y contingencia.
Planes de contingencia	Descripción de planes de emergencia
Descripción de las operaciones	Descripción detallada de los siguientes eventos: 1. Procedimiento seguro de emisión y revocación de certificados. 2. Medidas de control de acceso. 3. Procedimientos de respaldo y recuperación.
Interacción entre la CA y la RA del PSC	El documento cubre los procedimientos que involucren interacción entre la CA y RA

5.3.16. **Evaluación Personal**

5.3.16.1 **Objetivo:** Verificar que el PSC emplea personal calificado para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica, firma digital y los procedimientos de seguridad y de gestión, con el fin de minimizar los riesgos de errores humanos, robos o mal uso de los atributos del cargo.

5.3.16.2 **Descripción:** Se evaluará en conformidad al análisis de riesgos del PSC que el personal que maneja o tiene acceso a sistemas e información sensible cumpla al menos con las siguientes condiciones:

- Que tenga la calificación técnica o profesional requerida para el cargo o función que desempeña.
- Que tenga la experiencia mínima requerida para el cargo y función que desempeña.
- Que esté instruido en los procedimientos mínimos de seguridad que debe guardar en su función.

ES COPIA FIEL DEL ORIGINAL
Abog. Eddys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Secretaría General

Econ. Expidio Palacios
Secretario General

Se evalúa el procedimiento que utiliza el PSC para reclutar, seleccionar, evaluar y contratar personal crítico.

El personal de operaciones y sistemas no debería tener acceso a funciones de confianza, hasta que todos sus antecedentes hayan sido razonablemente verificados.

El personal que manejen información sensible, deben ser personal fijo, y deben existir contratos de confidencialidad que se extiendan más allá de la vigencia del contrato del empleado y/o empresa externa.

5.3.16.3 **Estándares de Evaluación**

- NP-ISO/IEC 27001. Anexo A. Dominio 7.
- ETSI TS 102 042

5.3.16.4 **Documentación Solicitada**

- Perfiles de los cargos del personal que maneja información o sistemas sensibles Currículos de las personas que ocupan los cargos y funciones sensibles.
- Evidencia de Identificación del personal calificado como crítico, durante la visita del personal designado por el MIC, en la forma que él lo solicite (Presentación de CV, foto, etc.)
- Manual de Procedimientos de administración de recursos humanos.

5.3.16.5 **Detalles de la Evaluación**

Aspectos	Evaluación
Experiencia profesional del personal crítico	Se valida la experiencia del personal crítico que trabaja para el PSC, verificando la concordancia de los perfiles en cada cargo y función, con el análisis de riesgos.
Capacitación del Personal crítico en aspectos de seguridad acorde a su función y cargo	Se confirma que el personal crítico esté capacitado en las prácticas de seguridad que debe observar de acuerdo a su cargo y función.
Procedimiento de contratación del personal crítico	Se valida el procedimiento definido por el PSC para la contratación del personal crítico.
Procedimiento de seguridad relacionado a RRHH	Se validan controles: • antes de la contratación, • durante la contratación y • cuando se produce cese o cambio de puesto de trabajo.

Abog. Rodys Rolón
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

MINISTERIO DE INDUSTRIA Y COMERCIO - Secretaría General -

Econ. Expidio Palacios
Secretario General

6. PROCEDIMIENTO DE HABILITACION

6.1. Procedimiento de Habilitación

A continuación se describe el procedimiento de la solicitud de habilitación, especificando los pasos y la relación entre el solicitante en constituirse en PSC y el MIC.

RESPONSABLE	ACCION
Solicitante (PSC)	1. Recaba en el sitio web (www.acraiz.gov.py) o en las oficinas de la DGFDyCE del MIC, sito Av. Mcal. López N° 3333 esq. Dr. Weiss, los requisitos técnicos y legales para obtener la habilitación como PSC. 2. Abona la/s tasa/s establecida/s por Resolución Ministerial correspondientes a la solicitud de habilitación, según liquidación generada por el MIC, previa presentación al MIC. 3. Presenta en mesa de entrada del MIC nota de solicitud acompañada del formulario de solicitud de habilitación firmado por el representante legal, los documentos y antecedentes de tipo: legal, técnico requeridos por la normativa y el comprobante de abono de tasa.
MIC	4. Recibe la solicitud de habilitación acompañada de las documentaciones y demás antecedentes de tipo: legal, técnico y comprobante de abono de tasa/s. 5.Verifica que las documentaciones y recaudos estén completos: a. Si están completos: i Admite a trámite la solicitud de habilitación ii Envía notificación al solicitante. iii Se pasa al paso 6 b. Si no están completos: i Se notifica al solicitante dentro del plazo de diez (10) días hábiles, otorgando la posibilidad de que el solicitante pueda completar las documentaciones faltantes o recaudos en el plazo de quince (15) días, bajo apercibimiento del rechazo de la solicitud. 6. Analiza, evalúa los documentos presentados y se notifica la fecha de inspección a las instalaciones.
Solicitante(PSC)	7. Abona la tasa de inspección de habilitación.
MIC	8. Realiza inspecciones técnicas a las instalaciones del solicitante, dentro del plazo de treinta (30) días hábiles contados desde la fecha de la admisibilidad de la solicitud plazo prorrogable una sola vez por igual periodo; con la posibilidad de solicitar documentación adicional. 9. Emite informe del resultado de la inspección: a. Si cumple con los requisitos ir al paso 12 b. Si no cumple: b.1 Y los incumplimientos son subsanables el MIC, comunica al solicitante el plazo en el cual deberán ser subsanados, ir al paso 10. b.2. Si los requisitos y obligaciones o el incumplimiento es insubsanable ir al paso 16:
Solicitante(PSC)	10. El solicitante debe subsanar los incumplimientos en el plazo señalado por el MIC e informar a éste una vez regularizados.
MIC	11. Fija fecha de nueva inspección para corroborar que se haya subsanado el incumplimiento. Ir a paso 6

Abog. Reys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Econ. Expidio Palacios
Secretario General

MIC	12. Una vez cumplido con los requisitos y obligaciones exigidas por la normativa se solicita la Póliza de Seguro exigida por la Ley 4017/2010, en el plazo de quince (15) días bajo apercibimiento de ser rechazada la solicitud.
SOLICITANTE (PSC)	13. Presenta la póliza de seguro dentro del plazo establecido.
MIC	14. Si la póliza cumple con los requerimientos establecidos emite informe final de habilitación. Si la póliza no cumple con los requisitos y obligaciones o no es presentada emite dictamen final de rechazo. Ir al paso 16 15. Dicta resolución ministerial de habilitación sustentado en un dictamen técnico–jurídico y se notifica al solicitante de la resolución y la fecha de generación del CSR y emisión de certificado. Ir al paso 17.
MIC	16. Emite resolución de rechazo sustentada en un dictamen técnico - jurídico y notifica al solicitante. Se puede recurrir la Resolución del rechazo, en lo contencioso, en un plazo de diez y ocho (18) días. Fin del proceso.
SOLICITANTE (PSC)	17. Genera el CSR en presencia de representantes del MIC en la fecha establecida por éste.
MIC	18. Emite Certificado en base al CSR generado por el PSC habilitado, en un plazo máximo de cinco (5) días hábiles a partir de la notificación de la resolución de habilitación.
SOLICITANTE (PSC)	19. Firma el Acuerdo de Suscriptor con el MIC. 20. Instala el certificado del PSC en su infraestructura tecnológica en presencia de representantes del MIC. 21. Finaliza el proceso.

6.2 **Lista de Recaudos**

Tabla N° 1 Recaudos Legales

LEGALES		
N°	**RECAUDO**	**OBSERVACION**
L01	**DOCUMENTOS PARA EL SOLICITANTE**	
L01.1	Personería y situación jurídica	Copia autenticada por escribanía
L01.2	Acta de Constitución de sociedad.	Copia autenticada por escribanía
L01.3	Acta de última asamblea.	Copia autenticada por escribanía
L01.4	Documento que acredite la representación legal invocada.	Copia autenticada por escribanía
L01.5	Certificado de cumplimiento tributario vigente.	Original o copia autenticada por escribanía
L01.6	Certificado vigente de no encontrarse en quiebra, convocatoria de acreedores o interdicción .	Original o copia autenticada por escribanía
L01.7	Constancia de estar al día con el seguro social.	Original o copia autenticada por escribanía.
L01.8	Capital mínimo de doscientos (200) salarios mínimos para actividades diversas no especificadas en la capital al momento de la habilitación.	Original o copia autenticada por escribanía

ES COPIA FIEL DEL ORIGINAL

Abog. Rocys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

MINISTERIO DE INDUSTRIA Y COMERCIO - Secretaría General -

Econ. Expidio Palacios
Secretario General

LEGALES		
N°	RECAUDO	OBSERVACION
L01.9	Certificados vigentes de antecedentes policiales y judiciales de sus representantes legales, administradores y funcionarios.	Original
L01.10	Contratos o acuerdos suscriptos con terceras personas que guarden relación con el servicio de certificación digital y la operativa.	Copia autenticada por escribanía
L01.11	Proforma de acuerdos de suscriptores.	Original
L01.12	Declaración de Prácticas de Certificación y Políticas de Certificación.	Original
L01.13	Póliza de Seguro	Original o copia autenticada.
L01.14	Comprobante de pago de tasa/s	Original o copia autenticada.

Tabla N° 2 Recaudos Técnicos

TECNICOS		
N°	RECAUDO	OBSERVACION
T00	DOCUMENTOS PARA EL SOLICITANTE	
T01	INFRAESTRUCTURA DE CLAVE PÚBLICA	
T01.1	Estructura del certificado digital	Modelo de Certificado digital y Modelo de la solicitud de firma del certificado (CSR)
T01.2	Estructura e información de la lista de Certificados digitales revocados (CRL)y servicio OCSP	Lista de Certificados Revocados (CRL) Certificado digital de la CA que la emite
T01.3	Registro de acceso público	Documento descriptivo que contenga al menos: detalle del sitio web donde se publicará la información, descripción de la tecnología, disponibilidad, accesibilidad, conexión, esquemas y diagramas de funcionamiento, medidas de seguridad y sitio web con funcionalidades requeridas
T02	SEGURIDAD	
T02.1	Evaluación de riesgos	Debe incluir el reporte de la valoración de riesgos y la estructura del proceso de valoración de riesgos
T02.2	Política de seguridad de la información	Debe estar basada en las recomendaciones del estándar NP ISO 27001:2014y en los anexos N° 2 y 4 de la presente Guía.
T02.3	Plan de continuidad del negocio y recuperación ante desastres	Debe estar basado en las recomendaciones del estándar ISO 27002:2013sección 17 y en el anexo N° 2 de la presente Guía.
T02.4	Plan de Seguridad de la información	Debe basarse en las recomendaciones del estándar ISO 27002:2013 y en el anexo 5 y 8 de la presente Guía.
T02.5	Plan de Administración de Claves Criptográficas	Debe estar basado en las recomendaciones del estándar ETSI TS 102 042 y FIPS PUB 140-2
T02.6	Documento de la Implementación de seguridad física y ambiental	Debe seguirse las recomendaciones del apartado de Seguridad física y ambiental de la Norma NP ISO 27002:2014 (contemplado en el dominio 11 del anexo 2 de la presente Guía).

TECNICOS		
N°	**RECAUDO**	**OBSERVACION**
T02.7	Acto administrativo de aprobación de Sistema de Prevención de Incendios aprobado por el municipio	Deben seguirse todas las recomendaciones de seguridad basadas en los principios y buenas prácticas de prevención de incendios.
T03	**PLATAFORMA TECNOLÓGICA**	
T03.1	Evaluación de la plataforma Tecnológica	Debe contemplar lo especificado en el Punto. 5.3.10 de la presente Guía.
T04	**POLÍTICAS DE CERTIFICACIÓN**	
T04.1	Declaración de Prácticas de Certificación y Política de Certificación	Debe seguirse las recomendaciones del estándar RFC 3647 y ETSI TS 102 042. Incluir la estructura de campos de los diferentes tipos de certificados a emitir. Debe presentar la CP para cada tipo de certificado
T04.2	Modelo de Operación de la Autoridad de Certificación (CA) del PSC	Debe contemplar lo especificado en el Anexo No. 6de la presente Guía.
T04.3	Modelo de Operación de la Autoridad de Registro (RA)	Debe contemplar lo especificado en el Anexo No. 7 de la presente Guía.
T05	**ADMINISTRACIÓN DE LOS SERVICIOS DE CERTIFICACIÓN**	
T05.1	Manual de Operación de la Autoridad de Certificación del PSC	Debe seguir las recomendaciones del estándar RFC 3647 y ETSI TS 102 042 y contemplar lo especificado en el apartado 5.3.14 de la presente Guía.
T05.2	Manual de Operación de la Autoridad de Registro	Debe seguir las recomendaciones del estándar RFC 3647 y contemplar lo especificado en el apartado 5.3.15 de la presente Guía.
T06	**MODELO ORGANIZACIONAL**	
T06.1	Estructura organizativa	Debe presentar la estructura organizativa del PSC, describiendo las unidades y cantidad de personas dedicadas a las labores relacionadas a la acreditación solicitada.
T06.2	Evaluación del personal	Debe seguir las recomendaciones del estándar ISO 27002:2013 y ETSI TS 102 042 y contemplar lo especificado en el apartado 5.3.16 de la presente Guía y presentar: -Perfiles de los cargos que manejan información o sistemas sensibles - CV de las personas que ocupan los cargos y funciones sensibles - Procedimientos de seguridad aplicados en la contratación - Identificación del personal calificado como crítico, durante la visita del representante del MIC, en la forma que el mismo lo solicite (CV, Foto, otros).

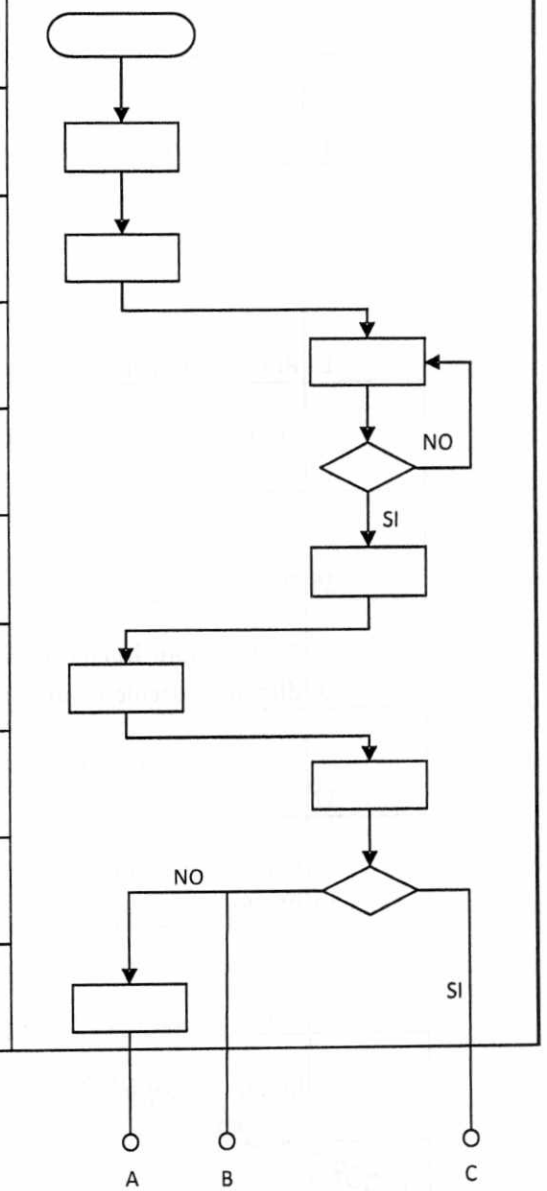
Abog. Rolys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

MINISTERIO DE INDUSTRIA Y COMERCIO - Secretaría General -

Econ. Expidio Palacios
Secretario General

6.3. Flujograma de Procedimiento de Solicitud de Habilitación

No.	(2) RESPONSABLE / (1) ACTIVIDAD	SOLICITANTE	MIC
1	Inicio		
2	Abona tasa de habilitación		
3	Presenta nota de solicitud		
4	Recibe solicitud		
5	¿Están completas las documentaciones?		
6	Analiza, evalúa los documentos presentados		
7	Abona la tasa de inspección de habilitación		
8	Realiza inspecciones técnicas		
9	¿Cumple con los requisitos?		
10	El solicitante debe subsanar los incumplimientos en el plazo señalado		

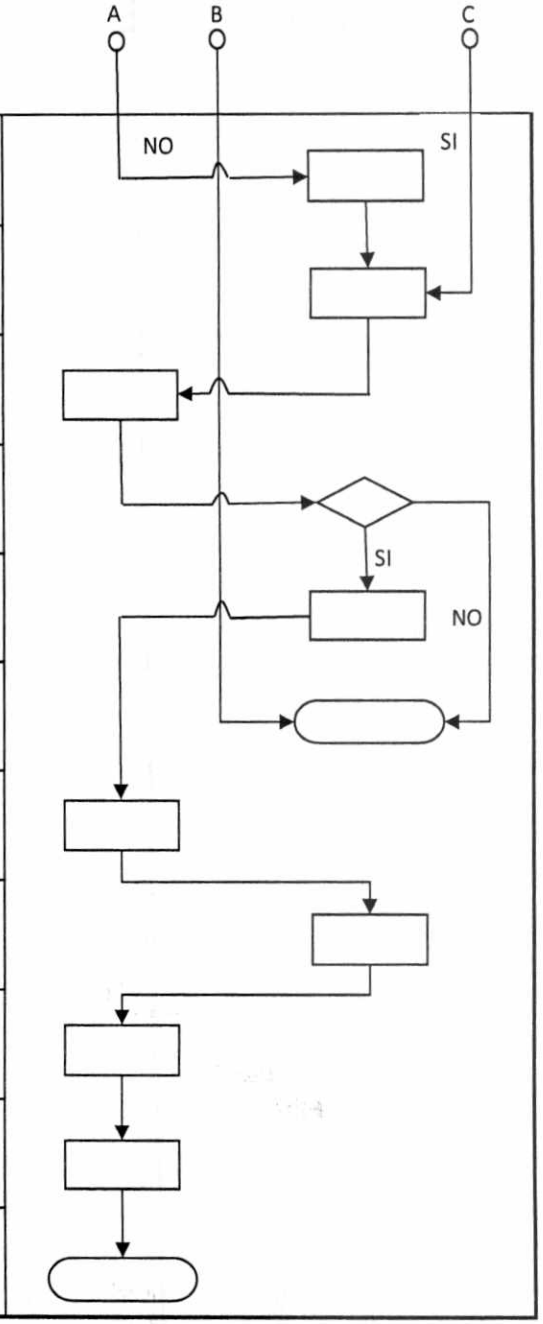


Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

MINISTERIO DE INDUSTRIA Y COMERCIO - Secretaría General

Econ. Expidio Palacios
Secretario General

11	Fija fecha de nueva inspección
12	Solicita la Póliza de Seguro exigida por la Ley
13	Presenta la póliza de seguro
14	¿La póliza cumple con los requerimientos establecidos?
15	Dicta resolución ministerial de habilitación
16	Emite resolución de rechazo sustentada en un dictamen técnico - jurídico
17	Genera el CSR en presencia de representantes del MIC
18	Emite Certificado en base al CSR generado por el PSC habilitado
19	Firma el Acuerdo de Suscriptor con el MIC
20	Instala el certificado del PSC en su infraestructura tecnológica
21	Fin



Abog. Rolys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Econ. Expidio Palacios
Secretario General

6.4. Contenido de Formulario de Solicitud de Habilitación

DATOS DEL SOLICITANTE DE LA PRESTACIÓN DE SERVICIO DE CERTIFICACIÓN								
Nombre o Razón Social:								
R.U.C. N°:					Capital Social:			
Domicilio/Calle:							N° de Casa:	
Ciudad:					Departamento:			
Sitio Web:								
Teléfono:								
Tipo de Entidad:	Pública		Privada				Consorciada	
	Nacional		Extranjera					
O.B.S.: * Si es consorciada completar formulario anexo. * Si es extranjera especificar país.								

DATOS DEL REPRESENTANTE LEGAL			
Nombre(s) y Apellido(s):			
Cédula de Identidad:		R.U.C. N°:	
Domicilio:			
Calle:			
Correo Electrónico (*)			
Nacionalidad:			
Teléfono:		Teléfono Celular:	

ACOMPAÑAR AL PRESENTE FORMULARIO LOS REQUISITOS ESTABLECIDOS EN EL ARTICULO N° 8 DEL DECRETO REGLAMENTARIO N° 7369 DEL 23 DE SETIEMBRE DE 2011.

(*) EL CORREO ELECTRÓNICO CONSIGNADO ES ACEPTADO EXPRESAMENTE COMO FORMA DE COMUNICACIÓN OFICIAL.

Firma y Sello del Funcionario – MIC
Aclaración de la Firma

Abog. Rolys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

MINISTERIO DE INDUSTRIA Y COMERCIO - Secretaría General

Firma del Solicitante
Aclaración de la Firma

Econ. Expidio Palacios
Secretario General

ANEXO DE LA EMPRESA MIEMBRO DEL CONSORCIO							
Nombre o Razón Social:							
R.U.C. N°:					Capital Social:		
Domicilio:							
Calle:							
Ciudad:					Departamento:		
Sitio Web:							
Teléfono:							
Tipo de Entidad:	Pública		Privada				
	Nacional		Extranjera				
O.B.S.: * Si es extranjera especificar país.							

ACOMPAÑAR AL PRESENTE FORMULARIO LOS REQUISITOS ESTABLECIDOS EN EL ARTICULO N° 8 DEL DECRETO REGLAMENTARIO N° 7369 DEL 23 DE SETIEMBRE DE 2011.

Firma del Solicitante

Aclaración de la Firma

Obs.: Tantos anexos como empresas contengan el consorcio.

ES COPIA FIEL DEL ORIGINAL

Abog. Rocío Rolón
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

MINISTERIO DE INDUSTRIA Y COMERCIO - Secretaría General -

Econ. Expidio Palacios
Secretario General

7. ANEXOS NORMATIVOS

Anexo N° 1

Ejemplo de Valoración de Riesgos

A continuación se presenta un cuadro de valoración solo como un ejemplo, para propósitos de guía.

Completar el siguiente cuadro de ejemplo de Valoración de Riesgo, identificando el activo, la posible amenaza, la posibilidad de que suceda, el daño en caso de ocurrir la amenaza, riesgo resultado, riesgo requerido y prioridad de la contramedida:

Identificación del activo	Amenaza al Activo	Posibilidad de ocurrencia de la Amenaza	Daño de ocurrir la amenaza	Riesgo resultado	Riesgo Requerido	Prioridad de la contra medida
Veracidad de la información pública disponible en el sitio web	Pérdida de confianza o buena fe debido a "hacking" de una página web	Alta	Menor	Medio	Bajo	1
Disponibilidad de servicio de correo externo	Ataque al servidor de correos tipo denegación de servicios (DoS)	Extrema	Dañino	Crítico	Bajo	4
Confiabilidad de sitio web	Falla accidental de equipo o suministro electrónico	Media	Grave	Crítico	Nulo	4
Acceso seguro a los servicios de red interna por personal autorizado, desde redes externas	Pérdida del token cripto gráfico o claves requeridas para acceder a los canales seguros	Muy baja	Serio	Medio	Bajo	1

Anexo Nº 2

Controles del Estándar NPISO/IEC 27001:2014, Secciones 5 a 18, Aplicables.

DOMINIO 5 Política de Seguridad

5.1 Orientación de administración para la seguridad de la información.

5.1.1 Políticas para la seguridad de la información.

5.1.2 Revisión de las políticas para la seguridad de la información.

ES COPIA FIEL DEL ORIGINAL

Abog. Rubys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

MINISTERIO DE INDUSTRIA Y COMERCIO
Secretaría General

Econ. Expidio Palacios
Secretario General

DOMINIO 6 Organización de la Seguridad de la información

6.1 Organización interna

6.1.1 Revisiones de los roles y responsabilidades de la seguridad en la información.

6.1.3 Contacto con las autoridades.

6.1.4 Contacto con grupos de interés especiales.

6.1.5 Seguridad de la información en la administración de proyectos.

6.2 Dispositivos para movilidad y teletrabajo.

6.2.1 Política de uso de dispositivos para movilidad.

6.2.2 Teletrabajo.

DOMINIO 7 Seguridad ligada a los recursos humanos

7.1 Antes del empleo

7.1.1 Selección.

7.1.2Términos y condiciones de empleo.

7.2 Durante el empleo

7.2.1 Responsabilidades de la Dirección.

7.2.2 Concientización, educación y capacitación sobre seguridad de la información.

7.2.3 Proceso disciplinario.

7.3 Despido o cambio de empleo

7.3.1 Despido o cambio de responsabilidades en el empleo.

DOMINIO 8 Gestión de activos

8.1 Responsabilidad por los Activos

8.1.1 Inventario de activos.

8.1.2 Propiedad de los activos.

8.1.3 Uso aceptable de activos.

8.1.4 Devolución de activos.

ES COPIA FIEL DEL ORIGINAL

Abog. Rocys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

MINISTERIO DE INDUSTRIA Y COMERCIO
Secretaría General

Econ. Expidio Palacios
Secretario General

8.2 Clasificación de la información

8.2.1 Clasificación de información.

8.2.2 Etiquetado de información.

8.2.3 Manejo de activos.

8.3 Manejo de medios

8.3.1 Administración de medios extraíbles.

8.3.2 Eliminación de medios.

8.3.3 Transferencia de medios físicos.

DOMINIO 9 Control de Accesos

9.1 Requisitos comerciales del control de accesos.

9.1.1 Política de control de acceso.

9.1.2 Acceso a redes y servicios de red.

9.2 Administración de accesos a los usuarios.

9.2.1 Registro y cancelación de registros de usuarios.

9.2.2 Entrega de acceso a los usuarios.

9.2.3 Administración de derechos de acceso privilegiado.

9.2.4 Administración de la información de autenticación secreta de los usuarios.

9.2.5 Revisión de los derechos de acceso de usuarios.

9.2.6 Eliminación o ajuste de los derechos de acceso.

9.3 Responsabilidades de los usuarios.

9.3.1 Uso de información confidencial para autenticación.

9.4 Control de accesos de sistemas y aplicaciones.

9.4.1 Restricción de acceso a la información.

9.4.2 Procedimientos de inicio de sesión seguros.

9.4.3 Sistema de administración de contraseñas.

9.4.4 Uso de programas de utilidad privilegiados.

9.4.5 Control de acceso al código de fuente del programa.

DOMINIO 10 Criptografía

10.1 Controles criptográficos

10.1.1 Políticas sobre el uso de controles criptográficos.

10.1.2 Administración de claves.

DOMINIO 11 Seguridad física y ambiental

11.1 Áreas seguras

11.1.1 Perímetro de seguridad física.

11.1.2 Controles de entrada física.

11.1.3 Protección de oficinas, salas e instalaciones.

11.1.4 Protección contra las amenazas externas y ambientales.

11.1.5 Trabajo en áreas seguras.

11.1.6 Áreas de entrega y carga.

11.2 Equipos

11.2.1 Emplazamiento y protección de equipos.

11.2.2 Servicios básicos de apoyo.

11.2.3 Seguridad del cableado.

11.2.4 Mantenimiento de equipos.

11.2.5 Retiro de activos.

11.2.6 Seguridad de los equipos y los activos fuera de las dependencias.

11.2.7 Eliminación o reutilización segura de equipos.

11.2.8 Equipos de usuario no supervisados.

11.2.9 Política de escritorio despejado y pantalla despejada.

DOMINIO 12 Seguridad física y ambiental

12.1 Procedimientos y responsabilidades operacionales

12.1.1 Procedimientos operativos documentados.

12.1.2 Administración de cambios.

Abog. Luis Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Econ. Expidio Palacios
Secretario General

12.1.3 Administración de capacidad.

12.1.4 Separación de entornos de desarrollo, pruebas y operacionales.

12.2 Protección contra malware

12.2.1 Controles contra el malware.

12.3 Respaldo

12.3.1 Respaldo de información.

12.4 Registro y monitoreo

12.4.1 Registro de eventos.

12.4.2 Protección del registro de información.

12.4.3 Registros del administrador y del operador.

12.4.4 Sincronización con relojes.

12.5 Control de software operacional

12.5.1 Instalación de software en sistemas operacionales.

12.6 Administración de vulnerabilidades técnicas

12.6.1 Administración de vulnerabilidades técnicas.

12.6.2 Restricciones en la instalación de software.

12.7 Consideraciones sobre la auditoría de los sistemas de información

12.7.1 Controles de auditoría de los sistemas de información.

DOMINIO13 Seguridad en las comunicaciones

13.1 Administración de la seguridad de redes

13.1.1 Controles de red.

13.1.2 Seguridad de los servicios de redes.

13.1.3 Segregación en las redes.

13.2 Transferencia de información

13.2.1 Políticas y procedimientos sobre la transferencia de información.

13.2.2 Acuerdos sobre la transferencia de información.

13.2.3 Mensajería electrónica.

13.2.4 Confidencialidad de los acuerdos de no divulgación.

ES COPIA FIEL DEL ORIGINAL

Abog. Edwin Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Secretaría General

Lcdo. Expidio Palacios
Secretario General

DOMINIO 14 Adquisición, desarrollo y mantenimiento de sistemas

14.1 Requisitos de seguridad de los sistemas de información

14.1.1 Análisis y especificación de los requisitos de seguridad de la información.

14.1.2 Protección de servicios de aplicación en redes públicas.

14.1.3 Protección de transacciones de servicios de aplicación.

14.2 Seguridad en los procesos de desarrollo y soporte

14.2.1 Política de desarrollo seguro.

14.2.2 Procedimientos de control de cambios del sistema.

14.2.3 Revisión técnica de las aplicaciones después de los cambios en la plataforma operativa.

14.2.4 Restricciones a los cambios de paquetes de software.

14.2.5 Principios de ingeniería segura del sistema.

14.2.6 Entorno de desarrollo seguro.

14.2.7 Desarrollo externalizado.

14.2.8 Pruebas de seguridad del sistema.

14.2.9 Pruebas de aceptación del sistema.

14.3 Datos de pruebas

14.3.1 Protección de los datos de pruebas.

DOMINIO 15 Relaciones con los proveedores

15.1 Seguridad de la información en las relaciones con los proveedores

15.1.1 Política de seguridad de la información para las relaciones con los proveedores.

15.1.2 Abordar la seguridad dentro de los acuerdos con los proveedores.

15.1.3 Cadena de suministro de la tecnología de información y comunicación.

15.2 Administración de prestación de servicios de proveedores

15.2.1 Monitoreo y revisión de los servicios del proveedor.

15.2.2 Administración de cambios en los servicios del proveedor.

ES COPIA FIEL DEL ORIGINAL

Abog. Dayis Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Secretaría General

Econ. Expidio Palacios
Secretario General

DOMINIO 16 Gestión de incidentes en la seguridad de la información.

16.1 Gestión de incidentes de seguridad de la información y mejoras

16.1.1 Responsabilidades y procedimientos.

16.1.2 Notificación de los eventos de seguridad de la información.

16.1.3 Notificación de puntos débiles de la seguridad.

16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.

16.1.5 Respuesta a los incidentes de seguridad.

16.1.6 Aprendizaje de los incidentes de seguridad de la información.

16.1.7 Recopilación de evidencias.

DOMINIO 17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.

17.1 Continuidad de la seguridad de la información.

17.1.1 Planificación de la continuidad de la seguridad de la información.

17.1.2 Implantación de la continuidad de la seguridad de la información.

17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

17.2 Redundancias

17.2.1 Disponibilidad de las instalaciones de procesamiento de la información.

DOMINIO 18 CUMPLIMIENTO

18.1 Cumplimiento de los requisitos legales y contractuales.

18.1.1 Identificación de la legislación aplicable.

18.1.2 Derechos de propiedad intelectual.

18.1.3 Protección de los registros de la organización.

18.1.4 Protección de datos y privacidad de la información personal.

18.1.5 Regulación de los controles criptográficos.

18.2 Revisiones de la seguridad de la información.

18.2.1 Revisión independiente de la seguridad de la información.

18.2.2 Cumplimiento de las políticas y normas de seguridad.

18.2.3 Comprobación del cumplimiento.

Econ. Expidio Palacios
Secretario General

Anexo N° 3

Contenido de la Declaración de Prácticas de Certificación (CPS) y Política de Certificación (CP)

1 INTRODUCCION

1.1 Descripción general

1.2 Nombre e Identificación del documento

1.3 Participantes de la PKI

1.3.1 Autoridades Certificadoras (CA).

1.3.2. Autoridad de Registro (RA).

1.3.3. Suscriptores.

1.3.4. Parte que confía.

1.3.5. Otros participantes.

1.4 Uso del Certificado

1.4.1 Usos apropiados del Certificado.

1.4.2. Usos prohibidos del certificado.

1.5 Administración de la Política

1.5.1. Organización que administra el documento.

1.5.2. Persona de Contacto.

1.5.3. Persona que determina la adecuación de la CPS a la Política

1.5.4 Procedimientos de aprobación de la Política de Certificación (CP).

1.6 Definiciones y acrónimos

1.6.1 Definiciones.

1.6.2 Acrónimos.

2 RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO

2.1. Repositorios.

2.2 Publicación de Información de Certificación.

2.3 Tiempo o frecuencia de Publicación.

2.4 Controles de Acceso a los Repositorios.

ES COPIA FIEL DEL ORIGINAL

Abog. Ramiro Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Econ. Expidio Palacios
Secretario General

3 IDENTIFICACIÓN Y AUTENTICACIÓN

3.1 Nombres.

3.1.1 Tipos de Nombres.

3.1.2. Necesidad de Nombres significativos.

3.1.3. Anonimato o seudónimos de los suscriptores.

3.1.4 Reglas para interpretación de varias formas de Nombres.

3.1.5 Unicidad de los nombres.

3.1.6 Reconocimiento, autenticación y rol de las marcas registradas.

3.2 Validación inicial de identidad.

3.2.1 Método para probar posesión de la clave privada.

3.2.2 Autenticación de identidad de Persona Jurídica.

3.2.3 Autenticación de identidad de Persona Física.

3.2.4 Información del Suscriptor no verificada.

3.2.5. Validación de la Autoridad (Capacidad de hecho).

3.2.6. Criterios para interoperabilidad.

3.3 Identificación y autenticación para solicitudes de re emisión de claves.

3.3.1 Identificación y autenticación para re emisión de claves rutinaria.

3.3.2 Identificación y autenticación para la re emisión de claves después de una revocación.

3.4 Identificación y autenticación para solicitudes de revocación.

4 REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

4.1 Solicitud del Certificado.

4.1.1 Quién puede presentar una solicitud de certificado.

4.1.2 Proceso de Inscripción y responsabilidades.

4.2 Procesamiento de la Solicitud del Certificado.

4.2.1 Ejecución de las funciones de Identificación y Autenticación.

4.2.2 Aprobación o rechazo de solicitudes de certificado.

4.2.3. Tiempo para procesar solicitudes de Certificado.

Abog. Rodrigo Roión A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

MINISTERIO DE INDUSTRIA Y COMERCIO
Secretaría General

Econ. Expidio Palacios
Secretario General

ES COPIA FIEL DEL ORIGINAL

Abog. Rolys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Secretaría General

Econ. Expidio Palacios
Secretario General

4.8.3 Procesamiento de solicitudes de modificación del certificado.

4.8.4 Notificación al suscriptor de la emisión de un nuevo certificado.

4.8.5 Conducta constitutiva de aceptación del certificado modificado.

4.8.6 Publicación por la CA de los Certificados modificados.

4.8.7 Notificación por la CA de emisión de certificado a otras entidades.

4.9 Revocación y suspensión.

4.9.1 Circunstancias para la revocación.

4.9.2 Quien puede solicitar Revocación.

4.9.3 Procedimiento para la solicitud de revocación.

4.9.4 Periodo de gracia para solicitud de revocación.

4.9.5 Tiempo dentro del cual la CA debe procesar la solicitud de revocación.

4.9.6 Requerimientos de verificación de revocación para las partes que confían.

4.9.7 Frecuencia de Emisión de la CRL.

4.9.8 Latencia máxima para CRLs.

4.9.9 Disponibilidad de verificación de revocación/estado en línea.

4.9.10 Requerimientos para verificar la revocación en línea.

4.9.11 Otras formas de advertencias de revocación disponibles.

4.9.12 Requerimientos especiales por compromiso de clave privada.

4.9.13 Circunstancias para suspensión.

4.9.14 Quien puede solicitar la suspensión.

4.9.15 Procedimiento para la solicitud de suspensión.

4.9.16 Límites del periodo de suspensión.

4.10 Servicios de comprobación de estado de Certificado.

4.10.1 Características operacionales.

4.10.2 Disponibilidad del Servicio.

4.10.3 Características opcionales.

4.11 Fin de la suscripción.

4.12 Custodia y recuperación de claves.

4.12.1 Política y prácticas de custodia y recuperación de claves.

Abog. Rocío Roldán A.
DIRECTORA GENERAL
Firma Digital y Comercio Electrónico

Econ. Expidio Palacios
Secretario General

4.12.2 Políticas y prácticas de recuperación y encapsulación de claves de sesión.

5 CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES

5.1 Controles físicos.

5.1.1 Localización y construcción del sitio.

5.1.2 Acceso físico.

5.1.3 Energía y Aire acondicionado.

5.1.4 Exposiciones al agua.

5.1.5 Prevención y protección contra fuego.

5.1.6 Almacenamiento de medios.

5.1.7 Eliminación de residuos.

5.1.8 Respaldo fuera de sitio.

5.2 Controles procedimentales.

5.2.1 Roles de confianza.

5.2.2 Número de personas requeridas por tarea.

5.2.3 Identificación y autenticación para cada rol.

5.2.4 Roles que requieren separación de funciones.

5.3 Controles de personal.

5.3.1 Requerimientos de experiencia, capacidades y autorización.

5.3.2 Procedimientos de verificación de antecedentes.

5.3.3 Requerimientos de capacitación.

5.3.4 Requerimientos y frecuencia de capacitación.

5.3.5 Frecuencia y secuencia en la rotación de las funciones.

5.3.6 Sanciones para acciones no autorizadas.

5.3.7 Requisitos de contratación a terceros.

5.3.8 Documentación suministrada al personal.

5.4 Procedimiento de Registro de auditoría.

5.4.1 Tipos de eventos registrados.

5.4.2 Frecuencia de procesamiento del registro.

ESCRIBIA FIEL DEL ORIGINAL

Abog. Rocío Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Econ. Expidio Palacios
Secretario General

5.4.3 Período de conservación del registro de auditoría.

5.4.4 Protección del registro de auditoría.

5.4.5 Procedimientos de respaldo de registro de auditoría.

5.4.6 Sistema de recolección de información de auditoría (interno vs externo).

5.4.7 Notificación al sujeto que causa el evento.

5.4.8 Evaluación de Vulnerabilidades.

5.5 Archivos de registros.

5.5.1 Tipos de registros archivados.

5.5.2 Periodos de retención para archivos.

5.5.3 Protección de archivos.

5.5.4 Procedimientos de respaldo de archivo.

5.5.5 Requerimientos para sellado de tiempo de registros.

5.5.6 Sistema de recolección de archivo (interno o externo).

5.5.7 Procedimientos para obtener y verificar la información archivada.

5.6 Cambio de clave.

5.7 Recuperación de desastres y compromiso.

5.7.1 Procedimiento para el manejo de incidente y compromiso.

5.7.2 Corrupción de datos, software y/o recursos computacionales.

5.7.3 Procedimientos de compromiso de clave privada de la entidad.

5.7.4 Capacidad de continuidad del negocio después de un desastre.

5.8 Terminación de una CA.

6 CONTROLES TÉCNICOS DE SEGURIDAD

6.1 Generación e instalación del par de claves.

6.1.1 Generación del par de claves.

6.1.2 Entrega de la clave privada al suscriptor.

6.1.3 Entrega de la Clave Pública al emisor del Certificado.

6.1.4 Entrega de la clave pública de la CA a las partes que confían.

6.1.5 Tamaño de la clave.

Es copia fiel del original
Ministerio de Industria y Comercio
Secretaría General

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Econ. Expidio Palacios
Secretario General

6.8 Sellado de tiempo (Time-stamping).

7 PERFILES DE CERTIFICADOS, CRL Y OCSP

7.1 Perfil del Certificado.

7.1.1 Número (s) de versión.

7.1.2 Extensiones del certificado.

7.1.2.1 Key Usage.

7.1.2.2 Extensión de política de certificados.

7.1.2.3 Nombre alternativo del sujeto.

7.1.2.4 Restricciones básicas.

7.1.2.5 Uso extendido de la clave.

7.1.2.6 Puntos de distribución de la CRL.

7.1.2.7 Identificador de clave de Autoridad.

7.1.2.8 Identificador de la clave del sujeto.

7.1.2.9 QcStatements.

7.1.3 Identificadores de objeto de algoritmos.

7.1.4 Formas del nombre.

7.1.5 Restricciones del nombre.

7.1.6 Identificador de objeto de Política de Certificado.

7.1.7 Uso de la extensión Restricciones de Política (Policy Constraints).

7.1.8 Semántica y sintaxis de los Calificadores de Política (Policy Qualifiers).

7.1.9 Semántica de procesamiento para la extensión de Políticas de Certificado (Certificate Policies).

7.2 Perfil de la CRL.

7.2.1 Número (s) de versión.

7.2.2 CRL y extensiones de entradas de CRL.

7.2.2.1 Número CRL (CRL Number).

7.2.2.2 Identificador de clave de Autoridad.

7.2.2.3 Puntos de distribución de las CRLs.

7.3 Perfil de OCSP.

ES COPIA FIEL DEL ORIGINAL

Abog. Edys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

MINISTERIO DE INDUSTRIA Y COMERCIO - Secretaría General

Econ. Expidio Palacios
Secretario General

7.3.1 Número (s) de versión.

7.3.2 Extensiones de OCSP

8. AUDITORIA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

8.1 Frecuencia o circunstancias de evaluación.

8.2 Identidad/calidades del evaluador.

8.3 Relación del evaluador con la entidad evaluada.

8.4 Aspectos cubiertos por la evaluación.

8.5 Acciones tomadas como resultado de una deficiencia.

8.6 Comunicación de resultados.

9. OTROS ASUNTOS LEGALES Y COMERCIALES

9.1 Tarifas.

9.1.1 Tarifas de emisión y administración de certificados.

9.1.2 Tarifas de acceso a certificados.

9.1.3 Tarifas de acceso a información del estado o revocación.

9.1.4 Tarifas por otros servicios.

9.1.5 Políticas de reembolso.

9.2 Responsabilidad financiera.

9.2.1 Cobertura de seguro.

9.2.2 Otros activos.

9.2.3 Cobertura de seguro o garantía para usuarios finales.

9.3 Confidencialidad de la información comercial.

9.3.1 Alcance de la información confidencial.

9.3.2 Información no contenida en el alcance de información confidencial.

9.4 Privacidad de información personal.

9.4.1 Plan de Privacidad.

9.4.2 Información tratada como privada.

9.4.3 Información que no es considerada como privada.

Abog. Rocío Holón A.
DIRECTORA GENERAL
Firma Digital y Comercio Electrónico

ES COPIA FIEL DEL ORIGINAL
MINISTERIO DE INDUSTRIA Y COMERCIO
Secretaría General

Econ. Expidio Palacios
Secretario General

9.4.4 Responsabilidad para proteger información privada.

9.4.5 Notificación y consentimiento para usar información privada.

9.4.6 Divulgación de acuerdo con un proceso judicial o administrativo.

9.4.7 Otras circunstancias de divulgación de información.

9.5 Derecho de Propiedad intelectual.

9.6 Representaciones y garantías.

9.6.1 Representaciones y garantías de la CA.

9.6.2 Representaciones y garantías de la RA.

9.6.3 Representaciones y garantías del suscriptor.

9.6.4 Representaciones y garantías de las partes que confían.

9.6.5 Representaciones y garantías de otros participantes.

9.7 Exención de garantía.

9.8 Limitaciones de responsabilidad legal.

9.9 Indemnizaciones.

9.10 Plazo y finalización.

9.10.1 Plazo.

9.10.2 Finalización.

9.10.3 Efectos de la finalización y supervivencia.

9.11 Notificación individual y comunicaciones con participantes.

9.12 Enmiendas.

9.12.1 Procedimientos para enmiendas.

9.12.2 Procedimiento de publicación y notificación.

9.12.3 Circunstancias en que los OID deben ser cambiados.

9.13 Disposiciones para resolución de disputas.

9.14 Normativa aplicable.

9.15 Adecuación a la ley aplicable.

9.16 Disposiciones varias.

9.16.1 Acuerdo completo.

9.16.2 Asignación.

9.16.3 Divisibilidad.

9.16.4 Aplicación (Honorarios de Abogados y renuncia de derechos).

9.16.5 Fuerza mayor.

9.17 Otras disposiciones.

10. DOCUMENTOS DE REFERENCIA

Anexo N° 4

Documento Estándar de una Política de Seguridad

Según la ISO 27002:2013, en el nivel más alto, las organizaciones deberían definir una "política de seguridad de la información" que la aprueba la dirección y que establece el enfoque de la organización para administrar sus objetivos de seguridad de la información.

Las políticas de seguridad de la información deberían abordar los requisitos creados por:

- Estrategia comercial;
- Normativas, legislación y contratos;
- El entorno de amenazas a la seguridad actual y proyectada.

La política de seguridad de la información debería tener enunciados respecto a lo siguiente:

- Definición de la seguridad de la información, los objetivos y principios para guiar a todas las actividades relacionadas con la seguridad de la información;
- Asignación de responsabilidades generales y específicas para la administración de la seguridad de la información de acuerdo a los roles definidos;
- Procesos para manejar desviaciones y excepciones.

A un nivel inferior, la política de seguridad de la información se debería respaldar por políticas específicas de un tema, que estipula la implementación de controles de seguridad de la información y que típicamente se estructura para abordar las necesidades de ciertos grupos objetivo dentro de una organización para abarcar ciertos temas.

Algunos ejemplos de dichos temas de políticas incluyen:

a) Control de accesos
b) Clasificación de la información (y manejo)
c) Seguridad física y ambiental
d) Temas orientados al usuario final como:
   - Uso aceptable de activos

ES COPIA FIEL DEL ORIGINAL

Abog. Rocys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Econ. Expidio Palacios
Secretario General

- Escritorio despejado y pantalla despejada
- Transferencia de información
- Dispositivos móviles y teletrabajo
- Restricciones sobre las instalaciones y el uso de software
- Respaldo

Anexo N° 5

Elementos de Evaluación de un Plan de Seguridad

La evaluación es una valoración de los siguientes aspectos:

- ¿Existe un administrador de la seguridad IT in situ?
- ¿Tiene el administrador de seguridad IT un conocimiento adecuado de su rol, consistente con aquel descrito en el Plan de Seguridad y el Manual de Operación?
- ¿Está el personal de soporte que se identifica en el Plan de Seguridad disponible?
- ¿Tiene el personal de soporte un conocimiento adecuado de su rol, consistente con aquel descrito en el Plan de Seguridad y el Manual de Operación?
- ¿Es el conjunto de signatarios privilegiados del sistema CA o RA consistente con el conjunto de signatarios privilegiados descritos en el plan de seguridad?
- ¿Está la infraestructura computacional y de red instalada y operando de acuerdo a lo descrito en: el Plan de Seguridad, el Manual de Operación, la CP y CPS y el Plan de Continuidad de Negocios y Recuperación ante Desastres?
- ¿Están los mecanismos de seguridad y procedimientos descritos en el Plan de Seguridad instalados y configurados o implementados de acuerdo con el Plan?

Se verificará principalmente:

1. Mecanismos de control de acceso
2. Captura y revisión de datos de Auditoría
3. Monitoreo de incidentes de seguridad
4. Administración de incidentes y procedimientos de respuesta ante incidentes.
5. Mantenimiento y uso de la información acerca de vulnerabilidades de las instalaciones de la CA o RA.
6. Plan de administración de claves criptográficas.
7. Administración de cuentas de suscriptores.
8. Control de medios removibles.

9. Respaldo y recuperación de datos y sistemas, incluyendo almacenamiento de segundas copias fuera de las instalaciones.
10. Control de inventario, incluyendo procedimientos de registro para controlar ubicación y acceso de los activos críticos.
11. Administración del Firewall internet.
12. Procedimientos y mecanismos que tengan un rol relevante en reducir las amenazas a las operaciones de la CA o RA.
13. Provee la confianza mediante la comprobación en terreno de que la seguridad operacional del PSC se mantendrá en el tiempo dadas las condiciones siguientes:
    - ¿Después que el grupo evaluador se ha retirado?
    - ¿Después de cambios en las amenazas de seguridad, personal, servicios ofrecidos, tecnología e infraestructura?

Anexo N° 6

Pauta de Modelo de Operación de la CA de un PSC

Este documento provee una guía para que un PSC documente el modelo de operaciones de la CA. El modelo de operaciones es uno de los primeros documentos que debieran ser preparados al iniciar sus actividades un PSC. El cual debería presentar una visión general de cómo interaccionarán los diferentes elementos constituyentes de un PSC.

Cubriendo aspectos operacionales, técnicos, legales, de seguridad y administración.

Algunas de las secciones de este documento pueden no aplicar a todos los PSC y la organización postulante debería presentar en la documentación aspectos que reflejen su circunstancia particular.

Resumen Ejecutivo

Presentar una visión general de las operaciones del PSC. Debiera responder a las siguientes preguntas:

¿Cuál es el producto y servicio?
¿Desde dónde se operará?
¿A quién se proveerá de certificados?
¿Quién estará involucrado en las operaciones?

ES COPIA FIEL DEL ORIGINAL

Abog. Rodrigo Rubén A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Econ. Expidio Palacios
Secretario General

Historia de la Empresa

Descripción breve de los orígenes de la organización, relaciones con los proveedores de tecnología y otras empresas asociadas.

Relaciones Comerciales

Proveer un resumen de las relaciones comerciales del PSC relación con las operaciones de la PKI. Si las operaciones involucran otras empresas, describir la relación con estas.

Prefacio del Documento

Describe el propósito y alcance del documento.
Descripción de los tópicos que cubre el documento y sus anexos.

Componentes del Sistema

Describe cuales son las partes funcionales del PSC, en sus distintos modos de operación.
Los componentes que se describen son los necesarios para operar el PSC y pueden incluir, pero no están limitados a: Interfaces entre la CA y RA, componentes de hardware y software.

Administración

Contiene las referencias a las políticas para los clientes, filosofía operacional, elementos estratégicos y de interrelación.
Se deben incluir detalles operacionales, como horarios de atención, personal requerido, infraestructura, etc.
Se puede incluir organigrama de la empresa.

Directorio

Describir brevemente: el estándar que utilice el directorio, por ejemplo x.500, la información incluida en el directorio y como afectan las revocaciones al directorio.

Bases de Datos de la CA

Describir brevemente la información que incluyen las bases de datos de la CA. Por ejemplo:

- Registro de ingreso y egreso a los sistemas
- Registro de la creación de certificados
- Detalles de los certificados
- Detalles de las revocaciones

Abog. Rodrigo Botón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

MINISTERIO DE INDUSTRIA Y COMERCIO - Secretaría General -

Econ. Expidio Palacios
Secretario General

Otros Subsistemas

- Cualquier otra información de subsistemas que pueda aplicar:
- Cuando se genera el par de claves, quien realiza esta función (CA/RA/suscriptor) Si el suscriptor genera las claves, indicar por cual medio y describir la tecnología utilizada.
- Medios de comunicación entre la CA y RA. Cuáles son las relaciones y dependencias entre ellas.
- Diagramas de los procesos pueden apoyar las descripciones.

Generación de Claves en la CA

Describir el proceso de generación de claves. Detalle de los mecanismos de protección de acceso para la generación de claves.

Generación de Certificados

Mostrar cómo opera la cadena de jerarquía. Incluir referencias al certificado raíz y las relaciones con otras CA si aplica.

Operaciones de la CA

Este punto debiera describir brevemente otros aspectos sensibles a la seguridad o de naturaleza sensible a las operaciones de la PSC y que no hayan sido descritos anteriormente.

Procedimientos de Recuperación de Datos

Presentar de manera breve la frecuencia de los respaldos y los procedimientos almacenamiento que se seguirán.

Planes de Auditoría

Describir cuales son los componentes del plan de Auditoría de la organización en cuanto a:

- Dispositivos de seguridad
- Seguridad
- Restricciones del personal
- Interfaces de administración

Recuperación de Desastres

Descripción de la estrategia para recuperación de desastres incluyendo:

- Definición de roles y responsabilidades
- Ejercicios de práctica para la recuperación de desastres, con cuanta frecuencia se realizan.

Abog. Rodrigo Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Econ. Expidio Palacios
Secretario General

- Respaldos en cinta, frecuencia, tipo de respaldo (por ejemplo incremental o total).
- Reiniciar el sistema.
- Procesos de Auditoría y generación de reportes.

Seguridad

Esta sección debe presentar brevemente todos los aspectos de seguridad que están involucrados en las operaciones de la CA y RA. Los detalles de estos aspectos pueden ser referenciados a otros documentos presentados.

Seguridad de las Instalaciones

Provee la descripción física del lugar donde operara la CA y RA.
Puede incluir referencias a otros documentos o procesos de certificación con los cuales cumpla.

Seguridad del Personal

Provee descripción de los requerimientos de seguridad para el personal de la organización, como por ejemplo:

- Referencia a que puestos pueden entrar en zonas restringidas
- Plan de entrenamiento para el personal
- Zonas restringidas para el personal
- Registro de ingresos
- Control de ingreso

Nivel de Seguridad del Módulo Criptográfico

Describe los productos y tecnología que se está utilizando para realizar las operaciones del PSC, en particular el módulo criptográfico de la CA.

Anexo N° 7

Pauta de Modelo de Operación de la RA de un PSC

Este documento provee una guía para que un PSC documente el modelo de operación de la RA.

El modelo de operación es uno de los primeros documentos que debieran ser preparados por el PSC al iniciar sus actividades. El cual debe presentar una visión general de cómo interaccionarán los diferentes elementos constituyentes de un PSC.

Abog. Rocío Rolón A.
DIRECTORA GENERAL
Firma Digital y Comercio Electrónico

MINISTERIO DE INDUSTRIA Y COMERCIO
Secretaría General

Econ. Expidio Palac.
Secretario General

Cubriendo aspectos operacionales, técnicos, legales, de seguridad y administración. Algunas de las secciones de este documento pueden no aplicar a todos los PSC y la organización postulante debe presentar en la documentación aspectos que reflejen su circunstancia particular.

Resumen ejecutivo

Debe presentar una visión general de las operaciones de la RA. Debe responder a las siguientes preguntas:

- ¿Cuál es el producto y servicio?
- ¿Desde dónde se operará?
- ¿A quién se proveerá de certificados?
- ¿Quién estará involucrado en las operaciones?

Historia de la Empresa

Descripción breve de los orígenes de la organización, relaciones con los proveedores de tecnología y otras empresas asociadas.

Relaciones Comerciales

Proveer un resumen de las relaciones comerciales del PSC en relación con las operaciones de la PKI.
Si las operaciones involucran otras empresas, describir la relación con estas.

Prefacio del Documento

Detalla el propósito y alcance del documento.
Descripción de los tópicos que cubre el documento y sus anexos.

Componentes Del Sistema

Describe cuales son los componentes funcionales de la RA, en sus distintos modos de operación.
Los componentes que se mencionen son los necesarios para operar el PSC y pueden incluir, pero no están limitados a: Interfaces entre la CA y RA, componentes de hardware y software.

Administración

Contiene las referencias a las políticas para los clientes o usuarios, filosofía operacional, elementos estratégicos y de interrelación.
Se deben incluir detalles operacionales, como horarios de atención, personal requerido, infraestructura, etc.
Se puede presentar organigrama de la empresa.

ES COPIA FIEL DEL ORIGINAL

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Econ. Expidio Palacios
Secretario General

Bases de Datos de la RA.

Describir brevemente la información que incluyen las bases de datos de la RA. Por ejemplo:

- Registro de ingreso y egreso a los sistemas
- Registro de la creación de certificados
- Detalles de los certificados
- Detalles de las revocaciones

Otros Subsistemas

Cualquier otra información de subsistemas que pueda aplicar:

- Como se registran los usuarios para obtener un certificado
- El medio usado para registrar.
- ¿Qué procesos se utilizan para registrar la identidad, y por quién?
- Cuando se genera el par de claves, quien realiza esta función (CA/RA/ suscriptor) Si el suscriptor genera las claves, indicar por cual medio y describir la tecnología utilizada.
- Medios de comunicación entre la RA y CA. Cuáles son las relaciones y dependencias entre ellas.

Generación de Claves en la RA

Describir el proceso de generación de claves. Cómo se comunica la RA y la CA una vez generadas las claves. Protección del mecanismo de generación de claves.

Operaciones de la RA

Este punto debe describir brevemente otros aspectos sensibles a las operaciones de la RA y que no hayan sido descritos anteriormente.

Procedimientos de respaldo y recuperación

Describir brevemente la frecuencia de los respaldos y los procedimientos de auditoría y almacenamiento que se seguirán.

Planes de Auditoría

- Describir cuales son los componentes del plan de Auditoría de la organización en cuanto a:
- Dispositivos de seguridad
- Seguridad
- Restricciones del personal
- Interfaces de administración

Recuperación de Desastres

- Descripción de la estrategia para recuperación de desastres incluyendo:
- Definición de roles y responsabilidades
- Ejercicios de práctica para la recuperación de desastres, con cuanta frecuencia se realizan.
- Respaldos en cinta, frecuencia, tipo de respaldo (por ejemplo incremental o total).
- Reiniciar el sistema.
- Procesos de Auditoría y generación de reportes.

Privacidad y entrenamiento

Describir brevemente:

- Las provisiones tomadas para proteger la información personal recolectada como evidencia de la identidad en el proceso de registro RA.
- Plan de entrenamiento del personal, en temas relacionados con el manejo de información privada y confidencial.

Seguridad

Esta sección debe describir brevemente todos los aspectos de seguridad que están involucrados en las operaciones de la RA. Los detalles de estos aspectos pueden ser referenciados a otros documentos presentados.

Seguridad de las Instalaciones

Provee la descripción física del lugar donde operará la RA. Puede incluir referencias a otros documentos o procesos de certificación con los cuales cumpla.

Seguridad del Personal

Describe los requerimientos de seguridad para el personal de la organización, como por ejemplo:

- Referencia a que puestos pueden entrar en zonas restringidas
- Plan de entrenamiento para el personal
- Zonas restringidas para el personal
- Registro de ingresos
- Control de ingreso

Nivel de seguridad del módulo criptográfico

Presenta los productos y tecnología que se está utilizando para realizar las operaciones del PSC, incluyendo el módulo criptográfico de la RA, si lo hay, y el dispositivo donde almacenará las claves el suscriptor.

Anexo N° 8

Controles físicos del centro de datos de las CA del PSC. Ubicación de las instalaciones

La infraestructura tecnológica de la CA, necesariamente deberá situarse dentro del territorio paraguayo, por tanto no podrá utilizar una infraestructura tecnológica establecida en el extranjero.

Las operaciones de la CA, deben estar dentro de un ambiente de protección física que impida y prevenga usos o accesos no autorizados o divulgación de información sensible. Las instalaciones de la CA deben contar con al menos seis perímetros de seguridad física:

- **Primer perímetro**: acceso a las instalaciones de la CA (área de recepción).
  Para acceder al primer perímetro de seguridad se requerirá que todo individuo sea identificado por el personal autorizado. En este perímetro no se realizará ninguna operación ni proceso administrativo de la CA.
- **Segundo perímetro:** acceso al área de procesos administrativos de la CA. Área interna al perímetro anterior, de acceso más estricto y restringido que el primero.
  Para acceder al segundo perímetro de seguridad se requerirá un factor de autenticación y tarjeta de identificación visible. En este perímetro, se desarrollan procesos administrativos de la CA.
- **Tercer perímetro:** acceso al área de operación de la CA. Área interna al perímetro anterior, de acceso más estricto y restringido que el segundo.
  Para acceder al tercer perímetro de seguridad se requerirán 2 factores (contraseña y tarjeta de proximidad). Solo podrán acceder a él, personal autorizado por la CA. En caso que se autorice el acceso a terceros, estos deben ir acompañados por, al menos un personal de la CA. En ésta área se desarrollan actividades como: servicios de soporte, climatización, energía, comunicaciones, monitoreo, validación de CSR (Solicitud de firma de certificado), publicación en el repositorio, entre otras.
- **Cuarto perímetro:** acceso al área de operaciones críticas de la CA. Área interna al perímetro anterior, de acceso más estricto y restringido que el tercero.
  Para acceder al cuarto perímetro de seguridad se requerirán 2 factores de autenticación como mínimo (al menos uno de ellos debe ser biométrico). Solo podrán acceder a él, personal autorizado por la CA. En caso que se autorice el acceso a terceros, estos deben ir acompañados por al menos dos personales de la CA. En ésta área se realizan actividades de emisión y revocación de certificados, emisión de CRL.

Abog. Rocío Polón A.
DIRECTORA GENERAL
Firma Digital y Comercio Electrónico

MINISTERIO DE INDUSTRIA Y COMERCIO - Secretaría General -

Econ. Expidio Palacios
Secretario General

- **Quinto perímetro:** acceso al área de resguardo de documentos y dispositivos sensibles. Área interna al tercer perímetro.
  El quinto perímetro de seguridad, constituye un recinto acorazado (cofre de seguridad), el acceso al mismo solo es permitido al personal autorizado. En ésta área se almacenan documentos y dispositivos sensibles inherentes a la operativa de la CA.
- **Sexto perímetro:** acceso al área de resguardo de clave privada. Área interna al cuarto perímetro.
  El sexto perímetro de seguridad, constituye un gabinete reforzado con cerraduras antirrobo (rack cofre), el acceso al mismo solo es permitido al personal autorizado. En ésta área se almacena la clave privada de la CA.

Abog. Rocio Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

ES COPIA FIEL DEL ORIGINAL

MINISTERIO DE INDUSTRIA Y COMERCIO - Secretaría General - REPÚBLICA DEL PARAGUAY

Econ. Expidio Palacios
Secretario General

JLRT/EP/pm